

BEST AVAILABLE COPY

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-313055

(43)Date of publication of application : 09.11.1999

(51)Int.Cl.

H04L 9/08

(21)Application number : 10-117088

(71)Applicant : HITACHI LTD

(22)Date of filing : 27.04.1998

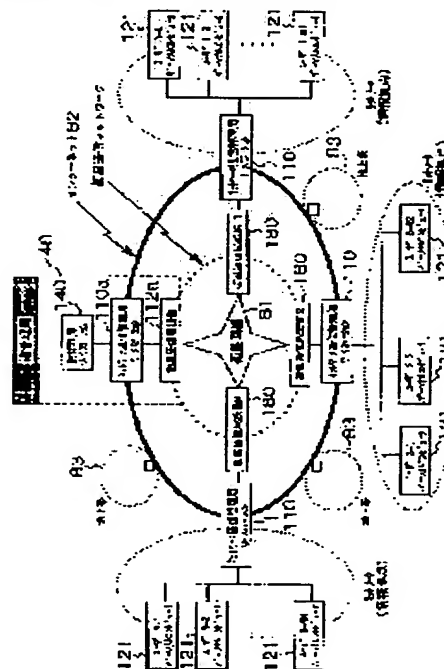
(72)Inventor : OGI HIROKAZU  
TAKASHIMA HIDEO  
TAKACHI MUNEHISA  
HAYAMIZU HIROSHI  
TANIGUCHI HIDENORI  
SHIRAKI MITSUHIKO

(54) CRYPTOGRAPHIC COMMUNICATION EQUIPMENT, DEVICE AND METHOD FOR  
MANAGING KEY, AND SYSTEM AND METHOD FOR NETWORK COMMUNICATION

(57)Abstract:

PROBLEM TO BE SOLVED: To secure the security of communication in a state of collecting groups composed of plural users into one system concerning cryptographic communication.

SOLUTION: A deciphering key for deciphering an enciphered sentence is previously applied to each work station 110, and the cryptographic key to be used for mutually transmitting data to a user 121 is determined from the relation ship of correspondence between the work station 110 and the deciphering key applied to this station, from the deciphering key, based on an identifier showing the user 121 at the destination, retrieved from a data base describing the relationship of correspondence between the work station 110 and a user 121 using this station, and from the relationship of correspondence between the cryptographic key and deciphering key.



## LEGAL STATUS

[Date of request for examination] 19.03.2002

[Date of sending the examiner's decision of rejection] 19.04.2005

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision] 2005-09384

of rejection]

[Date of requesting appeal against examiner's 19.05.2005  
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-313055

(43) 公開日 平成11年(1999)11月9日

(51) Int.Cl.<sup>6</sup>

H 0 4 L 9/08

識別記号

F I

H 0 4 L 9/00

6 0 1 D

6 0 1 E

審査請求 未請求 請求項の数12 O L (全 35 頁)

(21) 出願番号 特願平10-117088

(22) 出願日 平成10年(1998)4月27日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 扇 裕和

神奈川県横浜市戸塚区戸塚町216番地 株

式会社日立製作所宇宙技術推進本部内

(72) 発明者 高島 英雄

神奈川県横浜市戸塚区戸塚町216番地 株

式会社日立製作所宇宙技術推進本部内

(72) 発明者 高地 宗寿

神奈川県横浜市戸塚区戸塚町216番地 株

式会社日立製作所宇宙技術推進本部内

(74) 代理人 弁理士 富田 和子

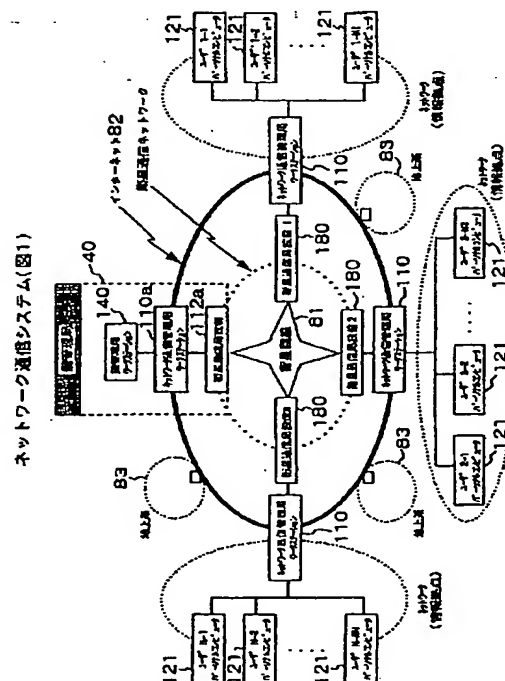
最終頁に続く

(54) 【発明の名称】 暗号通信装置、鍵管理装置および方法、ネットワーク通信システムおよび方法

(57) 【要約】

【課題】 複数のユーザから構成されるグループを暗号化通信に関する1つのまとまった系とした状態で、通信のセキュリティを確保する。

【解決手段】 各ワークステーション110に暗号文を復号化するための復号鍵を予め与え、ユーザ121相互にデータを伝送するに際して用いる暗号鍵を、ワークステーション110およびこれに与えられた復号鍵との対応関係、ならびに、ワークステーション110およびこれを用いるユーザ121の対応関係が記述されたデータベースから上記宛先のユーザ121を示す識別子に基づいて検索された復号鍵と、暗号鍵および復号鍵の対応関係とから決める。



## 【特許請求の範囲】

【請求項1】 各々複数のユーザが通信に用いることができる2以上のノードについて、各ノードに暗号文を復号化するための復号鍵を予め与え、ユーザ相互にデータを伝送するに際し、宛先のユーザが用いるノードに与えられた復号鍵に対応する暗号鍵を用いて暗号化通信を行うための鍵管理方法であって、

上記暗号化に用いられる暗号鍵は、上記宛先のユーザを示すユーザ識別子に基づいて、上記各ノードについて予め作成された、ノードを示すノード識別子および当該ノードに与えられた復号鍵との対応関係、ならびに、ノードを示すノード識別子および当該ノードを用いることができるユーザを示すユーザ識別子の対応関係が記述されたデータベースから検索された復号鍵と、暗号鍵および復号鍵の対応関係とから決められることを特徴とする鍵管理方法。

【請求項2】 各々複数のユーザが通信に用いることができる2以上のノードについて、各ノードごとに暗号文を復号化するための復号鍵を予め与え、ユーザ相互にデータを伝送するに際し、宛先のユーザが用いるノードに与えられた復号鍵に対応する暗号鍵を用いて暗号化通信を行うための鍵管理方法であって、

上記各ノードについて、ノードを示すノード識別子および当該ノードに与えられた復号鍵との対応関係、ならびに、ノードを示すノード識別子および当該ノードを用いることができるユーザを示すユーザ識別子の対応関係が記述されたデータベースを予め作成し、

発信元のユーザから、宛先のユーザを示すユーザ識別子を含む暗号化通信の要求を受け付け、

上記ユーザ識別子を用いて上記データベースから復号鍵を検索し、

上記検索した復号鍵と、暗号鍵および復号鍵の対応関係とから暗号鍵を決定し、

上記決定した暗号鍵を発信元のユーザが用いることができるノードに送付することを特徴とする鍵管理方法。

【請求項3】 各々複数のユーザが通信に用いることができる2以上のノードについて、各ノードごとに暗号文を復号化するための復号鍵を予め与え、

データを発信するに際し、宛先のユーザが用いるノードにおいて、送信すべきデータを第1の暗号鍵で第1の暗号アルゴリズムを用いて暗号化して暗号化データを生成し、上記第1の暗号鍵を、上記宛先のユーザが用いることができるノードに与えられた復号鍵に対応する第2の暗号鍵で第2の暗号アルゴリズムを用いて暗号化して暗号化暗号鍵を生成し、上記暗号化データおよび暗号化暗号鍵を送出し、

データを受信するに際し、宛先のユーザが用いるノードにおいて、受け付けたデータから暗号化暗号鍵および暗号化データを分離抽出し、当該ノードに与えられた復号鍵を用いて上記第2の暗号アルゴリズムに基づいて上記暗

号化暗号鍵を復号化して暗号鍵を取得し、該取得した暗号鍵を用いて上記第1の暗号アルゴリズムに基づいて暗号化データを復号化してデータを取得し、該取得したデータを受信ユーザに伝達し、

上記暗号鍵を暗号化するための暗号鍵は、データを発信するに際し、データを発信しようとするユーザから宛先のユーザを示す識別子を取得し、予め作成された、ユーザおよび復号鍵の対応を示すデータベースから検索された復号鍵と、暗号鍵および復号鍵の対応関係とから決定し、

上記データベースには、各ノードについて、ノードを示す識別子および当該ノードに与えられた復号鍵の対応関係、ならびに、ノードを示す識別子および当該ノードを用いることができるユーザの対応関係が予め登録されていることを特徴とする鍵管理方法。

【請求項4】 請求項3に記載の鍵管理方法において、上記第1の暗号アルゴリズムとして、秘密鍵暗号を用い、

上記第2の暗号アルゴリズムとして、公開鍵暗号を用いることを特徴とする鍵管理方法。

【請求項5】 請求項3に記載の鍵管理方法において、上記第1の暗号アルゴリズムとして、MULTI2を用い、

上記第2の暗号アルゴリズムとして、MULTI4を用いることを特徴とする鍵管理方法。

【請求項6】 暗号化／復号化機能を有し、各々複数のユーザが登録された通信サーバが2台以上接続されて構成されるネットワークで暗号化通信を行うためのネットワーク通信方法であって、

第1のユーザから第2のユーザにデータを伝送するに際し、

上記第1のユーザが登録されている第1の通信サーバに、上記第2のユーザが登録されている第2の通信サーバに予め与えられた復号鍵に対応する暗号鍵を与え、上記第1のユーザから第2のユーザに伝送されるべきデータを、上記第1の通信サーバにおいて上記与えた暗号鍵で暗号化した状態で送出し、

上記第2の通信サーバに到来したデータを当該第2の通信サーバに予め与えられた復号鍵で復号化することを特徴とするネットワーク通信方法。

【請求項7】 請求項6に記載のネットワーク通信方法において、

上記各通信サーバと通信することができる鍵管理サーバを設け、

上記鍵管理サーバに、上記各通信サーバを示すサーバ識別子と、各通信サーバに登録されたユーザを示すユーザ識別子と、各通信サーバに予め定められた復号鍵を示す復号鍵識別子とが記述されたデータベースを予め構築し、

上記通信サーバ相互にデータが伝送されるに際し、

発信元の通信サーバは、当該通信サーバを示すサーバ識別子、および、受信先ユーザを示すユーザ識別子を鍵管理サーバに与え、

上記鍵管理サーバは、上記与えられたユーザ識別子が示す受信先ユーザが登録されている通信サーバに与えられた復号鍵を上記データベースから検索し、当該検索した復号鍵に対応する暗号鍵を上記発信元のサーバに与えることを特徴とするネットワーク通信方法。

【請求項8】各々複数のユーザが登録された2以上の通信サーバが接続されて構成されるネットワーク通信システムであって、

上記各通信サーバは、

暗号鍵を管理するための鍵管理サーバと接続され、予め与えられた復号鍵で暗号文を復号化するための復号化機能と、上記鍵管理サーバから与えられた暗号鍵で暗号文を暗号化するための暗号化機能とを備え、

当該通信サーバに登録されているユーザからネットワーク上にデータを送出するに際し、データの宛先となるユーザの識別子を上記鍵管理サーバに与え、

上記鍵管理サーバは、上記与えられた識別子が示すユーザが登録されている通信サーバに予め与えられた復号鍵に対応する暗号鍵を、上記識別子を与えた通信サーバに与え、

上記暗号鍵を与えられた通信サーバは、送出すべきデータを上記与えられた暗号鍵で暗号化してネットワーク上に送出することを特徴とするネットワーク通信システム。

【請求項9】各々複数のユーザが登録された通信サーバが2以上接続されて構成されるネットワークにおける暗号化通信の暗号鍵を管理するための鍵管理装置であって、

ネットワーク上に接続される各通信サーバの識別子と、該各通信サーバに予め与えられた復号鍵との対応関係、および、各通信サーバの識別子と該各通信サーバに登録された複数のユーザとの対応関係が登録されたデータベースを備え、

通信サーバから送信先ユーザを示すユーザ識別子が与えられたとき、当該ユーザ識別子が示すユーザが登録された通信サーバに荒得られた復号鍵に対応する暗号鍵を、当該ユーザ識別子を与えた通信サーバに与えることを特徴とする鍵管理装置。

【請求項10】各々複数のユーザが登録された通信サーバが2以上接続されて構成されるネットワークにおける暗号化通信の暗号鍵を管理するための鍵管理装置であって、

ネットワークへのアクセス権を有する複数のユーザの識別子に、各ユーザがネットワークにアクセスする拠点となる通信サーバに予め与えられた復号鍵が対応づけて登録されたデータベースを備え、

通信サーバから宛先のユーザを示すユーザ識別子が与え

られたとき、当該ユーザ識別子に対応づけられた復号鍵に応じた暗号鍵を当該通信サーバに与えることを特徴とする暗号鍵管理装置。

【請求項11】ネットワークを介して暗号化通信を行うための暗号化通信装置であって、

双方向の通信を行うための通信手段と、

伝送すべき第1のデータを暗号化／復号化するための暗号化手段および復号化手段と、

上記第1のデータの伝送に先だって、第1のデータを暗号化するための暗号鍵を外部から取得するための暗号鍵取得手段とを備え、

上記暗号鍵取得手段は、第1のデータが伝送されるべき宛先のユーザを示す識別子を鍵管理のための情報処理装置に送出して、かつ、鍵管理のための情報処理装置から与えられる暗号鍵を受け付け、当該受け付けた暗号鍵を上記暗号化手段に与える機能を有することを特徴とする暗号化通信装置。

【請求項12】 請求項11記載の暗号化通信装置において、

上記暗号化手段および復号化手段における暗号アルゴリズムは、MULTI4暗号アルゴリズムであり、

上記第1のデータは、第2のデータがMULTI2暗号アルゴリズムで暗号化された際に用いられた暗号鍵であり、上記第2のデータと共に上記ネットワークを介して伝送されることを特徴とする暗号化通信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】データを、情報障害を避けた状態で伝送することに好適な、暗号通信装置、鍵管理装置および方法、ネットワーク通信システムおよび方法に係り、特に、ユーザが属するグループごとに鍵を管理することに好適な、暗号通信装置、鍵管理装置および方法、ネットワーク通信システムおよび方法に関する。

【0002】

【従来の技術】文書データ等の情報の伝達は、紙に印刷された書類の郵便、または公衆電話網を利用したFAXによる伝達が利用されている。

【0003】近年、パソコンの普及によりパソコンを公衆電話網に接続し、文書データそのものを電子メール、インターネット等により送受できるようになった。

【0004】情報伝達の安全性（セキュリティ）を確保する方法としては、文書作成を行うパソコンに暗号ソフトをインストールし、送受するユーザ間で伝達する文書を暗号化し通信する方法がとられる。

【0005】ユーザAとユーザBとが暗号化通信を行う場合、データを暗号化するための鍵と復号化するための鍵を定め、ユーザAは暗号化用の鍵でデータを暗号化し、これを受信したユーザBは復号化用の鍵で情報を復号化する。セキュリティを向上させるため、各ユーザがデータの暗号化、復号化に用いる鍵とは別の鍵をマスク

一鍵として所有し、情報伝達を実施するたびに、上記データの暗号化用の鍵と復号化用の鍵とをセッション鍵として生成し、ユーザAはユーザBにセッション鍵で暗号化したデータと、ユーザBが復号できるようユーザBのマスター鍵で暗号化したセッション鍵を送付する。

【0006】複数のユーザ間でネットワークを構築し、双方向の暗号化通信を行う場合は、専用の鍵管理局を設置して暗号に用いるマスター鍵、セッション鍵を管理すると共に、ユーザが所有するマスター鍵を利用してユーザの確認を行い、確認できないユーザのネットワーク利用を排除するアクセス管理が行われる。

【0007】

【発明が解決しようとする課題】ところが、上述した従来の技術では、暗号化通信が各ユーザ相互に、すなわち、マスター鍵、セッション鍵が各ユーザごとに運用される。このため、グループ間にまたがって暗号化通信が実施され、複数のユーザから構成されるグループを暗号化通信に関する1つのまとまった系とすることができない。

【0008】本発明は、複数のユーザから構成されるグループを暗号化通信に関する1つのまとまった系とした状態で、通信のセキュリティを確保することに好適な、暗号通信装置、鍵管理装置および方法、ネットワーク通信システムおよび方法を提供することにある。

【0009】

【課題を解決するための手段】上記目的を達成するために、本発明の第1の態様によれば、各々複数のユーザが通信に用いることができる2以上のノードについて、各ノードに暗号文を復号化するための復号鍵を予め与え、ユーザ相互にデータを伝送するに際し、宛先のユーザが用いるノードに与えられた復号鍵に対応する暗号鍵を用いて暗号化通信を行うための鍵管理方法であって、上記暗号化に用いられる暗号鍵は、上記宛先のユーザを示すユーザ識別子に基づいて、上記各ノードについて予め作成された、ノードを示すノード識別子および当該ノードに与えられた復号鍵との対応関係、ならびに、ノードを示すノード識別子および当該ノードを用いることができるユーザを示すユーザ識別子の対応関係が記述されたデータベースから検索された復号鍵と、暗号鍵および復号鍵の対応関係とから決められることを特徴とする鍵管理方法が提供される。

【0010】本発明の第2の態様によれば、各々複数のユーザが通信に用いることができる2以上のノードについて、各ノードごとに暗号文を復号化するための復号鍵を予め与え、ユーザ相互にデータを伝送するに際し、宛先のユーザが用いるノードに与えられた復号鍵に対応する暗号鍵を用いて暗号化通信を行うための鍵管理方法であって、上記各ノードについて、ノードを示すノード識別子および当該ノードに与えられた復号鍵との対応関係、ならびに、ノードを示すノード識別子および当該ノ

ードを用いることができるユーザを示すユーザ識別子の対応関係が記述されたデータベースを予め作成し、発信元のユーザから、宛先のユーザを示すユーザ識別子を含む暗号化通信の要求を受け付け、上記ユーザ識別子を用いて上記データベースから復号鍵を検索し、上記検索した復号鍵と、暗号鍵および復号鍵の対応関係とから暗号鍵を決定し、上記決定した暗号鍵を発信元のユーザが用いることができるノードに送付することを特徴とする鍵管理方法が提供される。

【0011】本発明の第3の態様によれば、各々複数のユーザが通信に用いることができる2以上のノードについて、各ノードごとに暗号文を復号化するための復号鍵を予め与え、データを発信するに際し、宛先のユーザが用いるノードにおいて、送信すべきデータを第1の暗号鍵で第1の暗号アルゴリズムを用いて暗号化して暗号化データを生成し、上記第1の暗号鍵を、上記宛先のユーザが用いることができるノードに与えられた復号鍵に対応する第2の暗号鍵で第2の暗号アルゴリズムを用いて暗号化して暗号化暗号鍵を生成し、上記暗号化データおよび暗号化暗号鍵を送出し、データを受信するに際し、宛先のユーザが用いるノードにおいて、受け付けたデータから暗号化暗号鍵および暗号化データを分離抽出し、当該ノードに与えられた復号鍵を用い上記第2の暗号アルゴリズムに基づいて上記暗号化暗号鍵を復号化して暗号鍵を取得し、該取得した暗号鍵を用い上記第1の暗号アルゴリズムに基づいて暗号化データを復号化してデータを取得し、該取得したデータを受信ユーザに伝達し、上記暗号鍵を暗号化するための暗号鍵は、データを発信するに際し、データを発信しようとするユーザから宛先のユーザを示す識別子を取得し、予め作成された、ユーザおよび復号鍵の対応を示すデータベースから検索された復号鍵と、暗号鍵および復号鍵の対応関係とから決定し、上記データベースには、各ノードについて、ノードを示す識別子および当該ノードに与えられた復号鍵の対応関係、ならびに、ノードを示す識別子および当該ノードを用いることができるユーザの対応関係が予め登録されていることを特徴とする鍵管理方法が提供される。

【0012】本発明の第4の態様によれば、暗号化/復号化機能を有し、各々複数のユーザが登録された通信サーバが2台以上接続されて構成されるネットワークで暗号化通信を行うためのネットワーク通信方法であって、第1のユーザから第2のユーザにデータを伝送するに際し、上記第1のユーザが登録されている第1の通信サーバに、上記第2のユーザが登録されている第2の通信サーバに予め与えられた復号鍵に対応する暗号鍵を与え、上記第1のユーザから第2のユーザに伝送されるべきデータを、上記第1の通信サーバにおいて上記与えた暗号鍵で暗号化した状態で送出し、上記第2の通信サーバに到来したデータを当該第2の通信サーバに予め与えられた復号鍵で復号化することを特徴とするネットワー

ク通信方法が提供される。

【0013】本発明の第5の態様によれば、各々複数のユーザが登録された2以上の通信サーバが接続されて構成されるネットワーク通信システムであって、上記各通信サーバは、暗号鍵を管理するための鍵管理サーバと接続され、予め与えられた復号鍵で暗号文を復号化するための復号化機能と、上記鍵管理サーバから与えられた暗号鍵で暗号文を暗号化するための暗号化機能とを備え、当該通信サーバに登録されているユーザからネットワーク上にデータを送出するに際し、データの宛先となるユーザの識別子を上記鍵管理サーバに与え、上記鍵管理サーバは、上記与えられた識別子が示すユーザが登録されている通信サーバに予め与えられた復号鍵に対応する暗号鍵を、上記識別子を与えた通信サーバに与え、上記暗号鍵を与えられた通信サーバは、送出すべきデータを上記与えられた暗号鍵で暗号化してネットワーク上に送出することを特徴とするネットワーク通信システムが提供される。

【0014】本発明の第6の態様によれば、各々複数のユーザが登録された通信サーバが2以上接続されて構成されるネットワークにおける暗号化通信の暗号鍵を管理するための鍵管理装置であって、ネットワーク上に接続される各通信サーバの識別子と、該各通信サーバに予め与えられた復号鍵との対応関係、および、各通信サーバの識別子と該各通信サーバに登録された複数のユーザとの対応関係が登録されたデータベースを備え、通信サーバから送信先ユーザを示すユーザ識別子が与えられたとき、当該ユーザ識別子が示すユーザが登録された通信サーバに荒得られた復号鍵に対応する暗号鍵を、当該ユーザ識別子を与えた通信サーバに与えることを特徴とする鍵管理装置が提供される。

【0015】本発明の第7の態様によれば、各々複数のユーザが登録された通信サーバが2以上接続されて構成されるネットワークにおける暗号化通信の暗号鍵を管理するための鍵管理装置であって、ネットワークへのアクセス権を有する複数のユーザの識別子に、各ユーザがネットワークにアクセスする拠点となる通信サーバに予め与えられた復号鍵が対応づけて登録されたデータベースを備え、通信サーバから宛先のユーザを示すユーザ識別子が与えられたとき、当該ユーザ識別子に対応づけられた復号鍵に応じた暗号鍵を当該通信サーバに与えることを特徴とする暗号鍵管理装置が提供される。

【0016】本発明の第8の態様によれば、ネットワークを介して暗号化通信を行うための暗号化通信装置であって、双方向の通信を行うための通信手段と、伝送すべき第1のデータを暗号化／復号化するための暗号化手段および復号化手段と、上記第1のデータの伝送に先だって、第1のデータを暗号化するための暗号鍵を外部から取得するための暗号鍵取得手段とを備え、上記暗号鍵取得手段は、第1のデータが伝送されるべき宛先のユーザ

を示す識別子を鍵管理のための情報処理装置に送出して、かつ、鍵管理のための情報処理装置から与えられる暗号鍵を受け付け、当該受け付けた暗号鍵を上記暗号化手段に与える機能を有することを特徴とする暗号化通信装置が提供される。

【0017】

【発明の実施の形態】以下、図面を参照して、本発明の実施の形態について説明する。

【0018】まず、図1を参照して、本発明を適用したネットワーク通信システムについて説明する。

【0019】図1において、複数のユーザで構成されるグループがN箇所存在するものとし、このグループ単位ごとに双方向の通信管理機能を持つネットワーク通信管理用ワークステーション（通信サーバ）110<1>～<N>を設置する。各ネットワーク通信管理用ワークステーション110<1>～<N>には、各グループに属するユーザがネットワークにアクセスするための情報処理装置120<1-1>～<1-M1>～<N-MN>（ただし、M1からMNは、各グループ（1～N）に属するユーザの数を示す。）が接続されている。情報処理装置120<1-1>～<1-M1>～<N-MN>は、各グループに属する複数のユーザによって情報処理装置端末として使用され、様々な情報処理装置が利用される。情報処理装置120<1-1>～<1-M1>～<N-MN>を上記ネットワーク通信管理用ワークステーション110<1>～<N>に接続し、ネットワーク通信システムが構築される。各ユーザは、上記通信ネットワークを利用して、文書データや、映像データを中心とする情報を双方向に伝達することができる。

【0020】このネットワーク通信管理用ワークステーション110<1>～<N>に衛星通信局設備112<1>～<N>を接続し、衛星通信回線81を介して各グループを結ぶと共に、上記ワークステーションをインターネット82に接続し、地上通信回線83と衛星通信回線81をあわせて、通信ネットワークを構築する。

【0021】ネットワーク通信管理用ワークステーション110<1>～<N>は、ユーザの要求に応じて伝達するデータの暗号化および復号化する機能とともに、1対1の個別配信や、同時にM箇所に配信する1:Mの同報通信機能を有し、暗号化による双方向通信を管理している。

【0022】このネットワーク通信システムには、鍵管理局40が設置されている。

【0023】鍵管理局40は他の情報拠点と同様に、衛星通信局設備112aとネットワーク通信管理用ワークステーション110aを所有しており、これに鍵管理を実施する鍵管理用ワークステーション140が接続し、暗号化通信に関与する鍵の管理を行っている。

【0024】ここで、図2を参照して、ネットワーク通信システムを利用するユーザの情報処理装置の接続例に



について説明する。各グループのユーザは様々な情報を生産し、使用する情報処理装置も多岐に渡っている。

【0025】図2において、使用される情報処理装置120としては、複数のユーザが使用しているパーソナルコンピュータ121、様々の設計・製造データの作成に使用するCAD用ワークステーション122、打ち合わせ等に使用するTV会議用パーソナルコンピュータ123、メールサーバ124等がある。

【0026】これらの情報処理装置とネットワーク通信管理用ワークステーションとは、LAN(local area network; ローカルエリアネットワーク)130で接続している。

【0027】鍵管理局40は、独立してネットワーク通信管理用ワークステーション110aを使用することもできるが、通信回線に余裕がある場合は、他のグループのユーザがルータ181を経由して、鍵管理局40のネットワーク通信管理用ワークステーション110aに接続することも可能である。

【0028】次に、図3を参照して、本発明を適用したネットワーク通信システムにおける、通信に関するデータの制御および処理について説明する。

【0029】この制御および処理は、各グループに設置されたネットワーク通信管理用ワークステーション、鍵管理局の鍵管理用ワークステーション、および各ユーザが使用するパーソナルコンピュータなどの情報処理装置により実施される。本発明を適用したネットワーク通信システムの通信に関する制御および処理は、大きく分けて、アクセス管理部1010と、ネットワーク通信管理部1020と、暗号化通信処理部1030と、鍵管理部1040と、否認防止管理部1050と、鍵回復部1060とを有して構成される。

【0030】上記アクセス管理部1010は、ユーザがパーソナルコンピュータ等の情報処理装置からネットワーク通信システムを利用しようとした場合、ユーザ認証として、システムからこのユーザに割り当てられているマスター鍵を所有しているかどうかの確認を実施し、ユーザの不正なアクセスを排除するアクセス管理を実施するためのものである。

【0031】上記ネットワーク通信管理部1020は、データを発信するユーザの要求に応じて、送受信設備を発信先の相手ユーザと接続し、ユーザの必要に応じて、1対1の個別配信または、同時にM箇所に配信する1:Nの同報通信を行うための送受信管理を実施するためのものである。

【0032】上記暗号化通信処理部1030は、発信するユーザ側で、伝達するデータを暗号化して送信し、受信側でこれを復号化してデータを取得する暗号化通信処理を実施するためのものである。

【0033】上記鍵管理部1040は、暗号化通信に関する鍵の生成、更新、削除、およびネットワーク利用

者に対する鍵の配布に関する鍵管理を実施するためのものである。

【0034】上記否認防止管理部1050は、ユーザが伝達するデータに対して、変造、偽造、不到達等の情報損失や、通信の当事者が実施した通信行為に対する否認を防止するための管理を実施するためのものである。

【0035】上記鍵回復部1060は、鍵の紛失、不正使用等、不測の事態が発生し通信された暗号文を解読する必要が生じた場合、鍵を回復し暗号文の復号を実施するためのものである。

【0036】次に、同じく図3を参照して、本発明のネットワーク通信システムにおける各制御処理部の処理の概要について説明する。ここでは、ユーザAからユーザBへ暗号化通信を行う場合をを例に挙げて説明する。

【0037】(1) ユーザAは、本発明のネットワーク通信システムにアクセスするため、使用するユーザが使用するパーソナルコンピュータの電源を投入する。すると、アクセス管理部1010が動作し、ユーザAが正当なユーザか否かを判断(確認)するためのユーザ認証を実施する。

【0038】正当なユーザと判断された場合、ユーザAは初めて、ネットワーク通信システムにアクセスすることが許可され、暗号化通信や送付されたデータを見ることが出来る。

【0039】(2) 暗号化通信を実施する場合、ユーザAはアクセス管理部1010に送信するデータと送信先相手の宛先を入力する。入力データと宛先とは、ネットワーク通信管理部1020に送られ、送信先相手と通信装置とを接続し、通信経路を確立する。

【0040】(3) データは、暗号化通信処理部1030に送られ、鍵管理部1040が発行した鍵を用いて暗号化され暗号文が作成される。作成された暗号文は、確立された通信経路に沿って送信先相手に伝達される。暗号文を受信した送信先相手は、鍵管理部1040が発行した鍵をもとにデータを復号し、取得したデータをネットワーク通信管理部1020に送付する。

【0041】(4) ユーザBに対してもアクセス管理部1010によりユーザ認証が実施され、ユーザBが正当なユーザと確認された場合、得られたデータはネットワーク通信管理部1020からアクセス管理部1010を経由してユーザBに伝達される。

【0042】(5) 鍵管理部1040は、暗号化通信処理部1030が使用する鍵のみならず、アクセス管理部1010がユーザ認証に使用する鍵についての管理、すなわち、鍵の登録、更新および削除を行う。

【0043】(6) ユーザAからユーザBに伝達されるデータに対して、否認防止に関する判定結果を必要とする場合、アクセス管理部1010に送信するデータを入力する際、同時に否認防止判定要求の入力を行う。

【0044】すると、否認防止管理部1050が動作



し、暗号化通信の前後で変造、偽造、不到達等の異常が発生したかどうかの判定を行う。

【0045】ユーザA、Bは、データ通信が終了してから否認防止管理部1050にアクセスすると、否認防止に関する判定結果を取得することができる。

【0046】(7) 不測の事態(例えば、鍵の紛失、不正使用等)が発生し、通常の暗号化通信経路によらず暗号文を復号する必要がある場合、鍵回復部1060に暗号文と鍵回復要求とを入力すると、暗号文を復号することができる。

【0047】本発明のネットワーク通信システムを構成するこの6つの制御処理は、ネットワーク通信システム上の各情報処理装置(例えば、図2に示される、各グループに設置されたネットワーク通信管理用ワークステーションとそれに接続するパーソナルコンピュータなどのユーザが使用する情報処理装置、および鍵管理局の鍵管理用ワークステーション)におけるソフト処理により実現される。

【0048】次に、図4を参照して、ユーザが使用するパーソナルコンピュータなどの情報処理装置、ネットワーク通信管理用ワークステーション、鍵管理用ワークステーションに組み込まれるソフト機能について説明する。

【0049】(1) ユーザが使用するパーソナルコンピュータなどの情報処理装置120は、ユーザセキュリティ機能f21と、データファイル処理機能f22とを備える。

【0050】上記ユーザセキュリティ機能f21は、ユーザのアクセス管理するためのユーザ認証の環境と、相手ユーザと接続するための操作環境とを提供するためのものである。

【0051】上記データファイル処理機能f22は、ユーザが個別または、同時に複数のユーザに対して、問い合わせ、伝達を行うための環境と、問い合わせ内容、伝達内容の設定、送信、回答結果の受信、回答結果の表示、および、任意のユーザにファイルを転送する操作環境とを提供するためのものである。

【0052】(2) ネットワーク管理用ワークステーション110は、通信セキュリティ管理機能f1と、ネットワーク送受信管理機能f12と、スクランブル機能f13と、デスクランブル機能f14と、通信構成管理機能f15とを備える。

【0053】上記通信セキュリティ管理機能f11は、ユーザからのユーザ認証要求に対する認証判定を暗号アルゴリズムにより実施し、また、相手ユーザと暗号化通信を実施する場合、暗号化通信要求が発生するごとに鍵管理ワークステーション140よりセッション鍵の受信し、暗号化通信を実施するためのものである。

【0054】上記ネットワーク送受信管理機能f12は、ネットワーク管理用ワークステーション110相互

に通信を実施するために、相手ユーザと接続し、通信経路の確立を行うためのものである。

【0055】上記スクランブル機能f13は、ネットワーク管理用ワークステーション110間で行われる通信において、送信データの暗号化と暗号化に必要な鍵の生成、およびこの鍵を配信するためのものである。

【0056】上記デスクランブル機能f14は、ネットワーク管理用ワークステーション110間で行われる通信において、受信データの復号化と、復号化に必要な鍵の受信およびこれを生成するためのものである。

【0057】上記通信構成管理機能f15は、ネットワーク管理用ワークステーション110で使用するデータベースの検索、登録、削除を行うためのものである。ネットワーク管理用ワークステーション110では、例えば、アクセスするユーザを管理するためのユーザIDデータベース11、ユーザ鍵管理データベース12を使用する。これらのデータベースの内容については後述する。

【0058】(3) 鍵管理用ワークステーション40は、鍵構成管理機能f41と、否認防止機能f42と、鍵回復機能f43とを備える。鍵管理用ワークステーション40では、例えば、ネットワークを使用するユーザを管理するためのネットワークユーザIDデータベース25、ネットワーク上の暗号化通信に用いる暗号鍵を管理するためのネットワーク鍵構成データベース24、および、否認を防止するための情報を格納した否認防止データベース(図示せず)を使用する。これらのデータベースの内容については後述する。

【0059】上記鍵構成管理機能f41は、暗号化通信に関与する鍵の発行、生成、更新、削除に関する鍵管理を実施するためのものである。

【0060】上記否認防止機能f42は、ユーザが実施するデータの送受信に対し、変造、偽造がなかったか、第3者としての公平な立場で、否認防止の判定を行うためのものである。

【0061】上記鍵回復機能f43は、鍵の紛失、不正使用という不測の事態が発生した場合、鍵を回復し通信に用いられる暗号文を復号するためのものである。

【0062】以下に、上記本発明のネットワーク通信システムの6つの制御処理部を、上記に示すコンピュータ、および、それに組み込まれたソフト機能で実現した実施例について説明する。

【0063】この実施例では、データの暗号化、復号化に用いるスクランブル鍵、デスクランブル鍵を運用する暗号アルゴリズムは、共通鍵暗号アルゴリズムを使用している。

【0064】ユーザに所有させるマスター鍵の生成、および、生成された鍵を配送するに際し使用する暗号アルゴリズムは、共通鍵暗号アルゴリズム、公開鍵暗号アルゴリズムのどちらでもシステムを構築することが可能で

ある。

【0065】まず、共通鍵暗号アルゴリズムを用いた実施例を示し、その後で、公開鍵暗号アルゴリズムを用いた実施例について説明する。

【0066】まず、図3、4および図5を参照して、共通鍵暗号アルゴリズムを用いた、アクセス管理部のソフト機能構成の実施例について説明する。

【0067】共通鍵暗号アルゴリズムとしては、例えば、MULTI4暗号アルゴリズムなどを用いることができる。MULTI4暗号アルゴリズムは、アルゴリズム決定鍵およびデータ鍵に基づき暗号化/復号化関数の決定を行う処理と、データの暗号化/復号化を行う処理との2段階に分けられた暗号処理を行う。この処理の内容については、例えば、特開平04-170576号公報などに記載されている。

【0068】図4において、アクセス管理部1010（図3参照）を運用するため、パーソナルコンピュータなどの情報処理装置120を使用する各ユーザには、あらかじめ鍵管理局40より、ユーザIDとマスター鍵としての秘密鍵が割り当てられている。

【0069】このユーザIDは、ネットワーク通信管理用ワークステーション110のユーザIDデータベース11に登録し、マスター鍵としての秘密鍵は、ネットワーク通信管理用ワークステーション110のユーザ鍵管理データベース12に、ユーザIDと対応させてユーザのマスター鍵として登録している。

【0070】アクセス管理部1010（図3参照）では、ユーザが使用するパーソナルコンピュータなどの情報処理装置120のユーザセキュリティ機能f21とネットワーク通信管理用ワークステーション110の通信セキュリティ機能f11との暗号化通信によって、ユーザ認証を実施する。

【0071】以下、図5を参照して、この実施例について説明する。

【0072】(1) ユーザが、本ネットワーク通信システムを利用する場合、ユーザが使用するパーソナルコンピュータなどの情報処理装置120にアクセス要求501を入力する。ユーザセキュリティ機能f21は、「シーケンス番号」505を付加しユーザ認証要求503として通信セキュリティ機能f11に送付する。

【0073】(2) この要求を受けて、通信セキュリティ機能f11は「ユーザID」506をキーとしてユーザIDデータベース11を検索し、「ユーザID」506が該当すれば、まず、時刻情報（「月」、「日」、「時」、「分」、「秒」）と乱数から構成される、チャレンジコードCAC<sub>0</sub>507を生成し、次に「ユーザID」506をキーとして、ユーザ鍵管理データベース12を検索し当該ユーザに割り当てられた「ユーザマスター鍵」P<sub>ID</sub>508を取得する。

【0074】そして、この「ユーザマスター鍵」P<sub>ID</sub>50

8によりチャレンジコードCAC<sub>0</sub>507を暗号化し暗号化チャレンジコードE<sub>PID</sub>（CAC<sub>0</sub>）509を作成し、ユーザセキュリティ機能f21に送付する。

【0075】(3) ユーザは、フロッピーディスクまたはICカードなどの記憶媒体に、当該ユーザに割り当てられたユーザマスター鍵508を保管しており、この鍵を入力することにより、送付された暗号化チャレンジコードE<sub>PID</sub>（CAC<sub>0</sub>）509を復号しチャレンジコードCAC510を生成する。

【0076】そして、この生成したチャレンジコードCAC510を通信セキュリティ機能に送り返す。

【0077】(4) 通信セキュリティ機能f11は、この機能で生成されたチャレンジコードCAC<sub>0</sub>507と復号されて送付されたチャレンジコードCAC510とを比較し、両者が一致すれば、ユーザを正当なユーザと判断し、認証判定結果を認証完了とする。逆に、両者が一致しなければ、認証判定結果を認証エラーとし、この認証判定結果をユーザセキュリティ機能f21に送付する。

【0078】(5) ユーザセキュリティ機能f21は、認証判定結果がユーザ認証完了の場合、「シーケンス番号」505を除いてユーザ認証結果としネットワーク通信管理部に伝達する。

【0079】次に、図4を参照して、ネットワーク通信管理部1020（図3参照）のソフト機能構成の実施例について説明する。

【0080】図4に示される、ユーザは使用するパーソナルコンピュータなどの情報処理装置120のデータファイル処理機能f22にデータを入力し、この機能から入力されたデータはネットワーク通信管理用ワークステーション110のネットワーク送受信管理機能f12に送られる。このネットワーク通信管理用ワークステーション110でユーザの要求に応じてデータが処理され送信先相手側に送付され、ネットワーク通信管理用ワークステーション110のネットワーク送受信管理機能f12を経由して、送信先相手ユーザに伝達される一連の処理がネットワーク通信管理部によって管理される。

【0081】以下、図3、4を参照して、このネットワーク通信管理部の実施例について説明する。

【0082】(1) ユーザが同時に複数のユーザに対して問い合わせを行う場合、

(i) ユーザが起動指示を行い、問い合わせ内容作成要求をデータファイル処理機能f22に入力する。

【0083】(ii) ウィンドウ画面上に入力画面が表示され、問い合わせ内容、および宛先が入力可能となる。

【0084】(iii) 問い合わせ内容送信要求を入力すると、ネットワーク送受信管理機能f12に同報データとして送付し、データ識別子を付加して暗号化通信処理部1030に送付する。

【0085】(2) ユーザが同時に複数のユーザに対して、回答を行う場合、

(i) ユーザが起動指示を行い、回答内容作成要求をデータファイル処理機能f22に入力する。

【0086】(ii) ウィンドウ画面上に入力画面が表示され、回答内容、および宛先を入力が入力可能となる。

【0087】(iii) 回答送信要求を入力すると、ネットワーク送受信管理機能f12に回答データとして送付し、データ識別子を付加して、暗号化通信処理部1030に送付する。

【0088】(3) ユーザが同時に複数のユーザに対して伝達を行う場合、

(i) ユーザが起動指示を行い、伝達内容作成要求をデータファイル処理機能f22に入力する。

【0089】(ii) ウィンドウ画面上に入力画面が表示され、伝達内容、および宛先が入力可能となる。

【0090】(iii) 伝達内容送信要求を入力すると、ネットワーク送受信管理機能f12に伝達データとして送付し、データ識別子を付加して、暗号化通信処理部1030に送付する。

【0091】(4) ユーザが同時に複数のユーザに対してファイル転送を行う場合、

(i) ユーザが起動指示を行い、ファイル転送要求をデータファイル処理機能f22に入力する。

【0092】(ii) ファイル名および宛先を入力すると、データベースからファイルが読み込まれる。

【0093】(iii) ネットワーク送受信管理機能f12にファイル転送データとして送付し、暗号化通信処理部1030に送付する。

【0094】以上のシーケンスで、問い合わせ内容の設定、送信、回答内容の設定、送信、伝達内容の設定、送信、転送ファイルの設定、送信が実施され、画面上に送信内容が表示される。問い合わせ内容の受信、回答結果の受信、伝達内容の受信、転送ファイルの受信も同様のシーケンスで実施され、画面上には、受信内容が表示される。

【0095】次に、図6を参照して、共通鍵暗号アルゴリズムを使用した場合の暗号化通信処理部のソフト機能構成の実施例について説明する。

【0096】暗号化通信を実施する場合、図4のネットワーク通信システムに組み込まれるソフト機能に示すように、ネットワーク通信管理用ワークステーション110のスクランブル機能は、ネットワーク送受信管理機能から送信するデータを受け取る。次に、鍵管理用ワークステーションの鍵構成管理機能からセッション鍵の発行を受け、この鍵をもとに受け取ったデータを暗号化し暗号文を作成し、送信先相手ユーザ側のネットワーク通信管理用ワークステーションのデスクランブル機能に送信する。

【0097】デスクランブル機能は、送付された暗号文を復号化し、データを取得する。

【0098】暗号化通信処理部を運用する前提条件として前述のアクセス管理部と同様、パーソナルコンピュータなどの情報処理装置を使用する各ユーザには、鍵管理局よりユーザIDとマスター鍵としての秘密鍵が割り当てられており、鍵管理用ワークステーションのネットワーク鍵構成データベースに、ユーザに割り当てたマスター鍵をユーザIDと対応させて登録し管理している。同様にネットワーク通信管理用ワークステーションのユーザ鍵管理データベースにユーザIDとマスター鍵とを対応させて登録しているものとする。

【0099】以下に、この暗号化通信処理部の実施例について説明する。

【0100】(1) 暗号化通信要求が発生すると、鍵管理用ワークステーション140の鍵構成管理機能f41は、セッション鍵 $P_T601$ を生成する。次に、送信側のユーザのマスター鍵 $P_{ID}602$ 、受信側のユーザのマスター鍵 $P_{ID}603$ をネットワーク鍵構成データベース24より取り出し、セッション鍵 $P_T601$ を平文として暗号化を行い、暗号文 $E_{PID}(P_T)604$ 、 $E_{PID}(P_T)605$ を作成する。この暗号文を発信側ユーザの使用するパーソナルコンピュータなどの情報処理装置と接続するネットワーク通信管理用ワークステーション110に送付する。

【0101】(2) 発信側のユーザの接続するネットワーク通信管理用ワークステーション110では、管理しているユーザのマスター鍵 $P_{ID}603$ をユーザ鍵管理データベース12より取り出し、この鍵を用いて、暗号化されて送付されたセッション鍵を復号し、セッション鍵 $P_T$ を取得する。

【0102】(3) 一方、発信側のユーザの接続するネットワーク通信管理用ワークステーション110では、ユーザが入力したデータMをネットワーク送受信管理機能f12から受け取り、このデータMを暗号化するためのスクランブル鍵 $K_S606$ 、復号化するためのデスクランブル鍵 $K_D607$ を生成する。

【0103】(4) 次に、ユーザが入力したデータMをスクランブル鍵 $K_S606$ で暗号化し、暗号文 $E_{KS}(M)608$ を作成し、同様にデスクランブル鍵 $K_D607$ をセッション鍵 $P_T$ で暗号化し、暗号文 $E_{PT}(K_S)609$ を作成する。この作成した2組の暗号文と、送付された暗号文 $E_{PID}(P_T)605$ とを送信先相手のユーザの使用するパーソナルコンピュータなどの情報処理装置が接続するネットワーク通信管理用ワークステーション110に送信する。

【0104】(5) 送信先相手ユーザ側のネットワーク通信管理用ワークステーション110は、このユーザのマスター鍵 $P_{ID}603$ をユーザ鍵管理データベース12より取り出し、この鍵を用いて送付された暗号化セッ

セッション鍵 $E_{PYID}(P_I)$  605を復号し、セッション鍵 $P_I$  601を取得する。次に、送付された暗号化デスクランブル鍵 $E_{P_I}(K_D)$  608を上記取得したセッション鍵 $P_I$  601を用いて復号し、デスクランブル鍵 $K_D$  607を取得する。

【0105】最後に、このデスクランブル鍵 $K_D$  607を用いて送付されたデータの暗号文 $E_{KS}(M)$  608を復号し、データ $M$ を取得する。

【0106】(6) 取得したデータは、ネットワーク送受信管理機能を經由して送信先相手ユーザに伝達される。

【0107】以上の方式で、ユーザからユーザへの暗号化通信を実施する。スクランブル鍵 $K_S$  606、デスクランブル鍵 $K_D$  607を運用するアルゴリズムとして、CSデジタル放送で実績のあるMULTI2暗号アルゴリズムを使用し、マスター鍵602、603およびセッション鍵601を運用するアルゴリズムとして、MULTI2とは異なるMULTI4の暗号アルゴリズムを用いるものとする。

【0108】このようにして、データの暗号化に用いるスクランブル鍵 $K_S$  606の暗号アルゴリズムと、デスクランブル鍵 $K_D$  607の配送に用いるセッション鍵601の暗号アルゴリズムとを、異なった暗号アルゴリズムとする二重暗号化方式を取ることが可能となる。従って、同一の暗号アルゴリズムを使用する場合とくらべてセキュリティの向上を図ることができる。

【0109】次に、図7を参照して、本発明を適用したネットワーク通信システムの鍵管理部のソフト機能構成の実施例について説明する。

【0110】鍵管理部1040(図3参照)は、アクセス管理部1010(図3参照)、暗号化通信処理部1030(図3参照)の実施例で述べたように、本ネットワーク通信システムを使用する全てのユーザのマスター鍵および、暗号化通信に関与するセッション鍵を管理しており、鍵管理用ワークステーション140のネットワーク鍵構成データベース24に全てのユーザのマスター鍵をユーザIDに対応させて登録している。

【0111】また、ネットワーク通信管理用ワークステーション110のユーザ鍵管理データベース12には、このネットワーク通信管理用ワークステーション110と接続するユーザのマスター鍵をユーザIDに対応させて登録している。

【0112】以下、図7を参照して、この鍵管理部の実施例について説明する。

【0113】(1) セッション鍵の管理

(i) 暗号化通信処理部1030(図3参照)で暗号化通信を行う場合、発信側ユーザのネットワーク通信管理用ワークステーション110の通信セキュリティ管理機能f11から、発信側のユーザIDと送信先相手のユーザIDを付加したセッション鍵発行要求701が、鍵

管理ワークステーション140の鍵構成管理機能f41に送付される。

【0114】(ii) 鍵構成管理機能f41は、この要求を受けセッション鍵 $P_I$ を生成するとともに、ユーザIDをキーとしてネットワーク鍵構成データベース24を検索し、発信側ユーザのマスター鍵 $P_{ID}$ 、送信先相手ユーザのマスター鍵 $P_{YID}$ を取り出す。次に、 $P_I$ を平文として暗号化し、暗号化セッション鍵 $E_{PID}(P_I)$ 、 $E_{PYID}(P_I)$ を作成し、発信側ユーザのネットワーク通信管理用ワークステーション110の通信セキュリティ管理機能f11に発行する。

【0115】(iii) 暗号化セッション鍵を受信した通信セキュリティ管理機能f11は、発信側ユーザのユーザIDをキーとしてユーザ鍵管理データベース12を検索し、ユーザのマスター鍵 $P_{ID}$ を取り出す。次に、このマスター鍵をもとに暗号化セッション鍵 $E_{PID}(P_I)$ を復号化し、セッション鍵 $P_I$ を取得する。

【0116】以上のシーケンスにより、発信側のユーザが接続するネットワーク通信管理用ワークステーション110に、セッション鍵 $P_I$ と暗号化セッション鍵 $E_{PYID}(P_I)$ が発行される。

【0117】(2) マスター鍵の管理

ユーザのマスター鍵は、鍵管理用ワークステーション140の鍵構成管理機能f41と、ネットワーク通信管理用ワークステーション110の通信構成管理機能f15により管理されており、ユーザのマスター鍵の登録、更新、削除はこれらの機能により実施される。

【0118】ネットワーク通信管理用ワークステーション110設置時、このワークステーションにネットワークIDとネットワークマスター鍵を割り当て、通信構成管理機能f15によりユーザ鍵管理データベース12に登録するとともに、鍵管理用ワークステーション140の鍵構成管理機能f41よりネットワーク鍵構成データベース24に登録する。

【0119】各ユーザのマスター鍵は、鍵構成管理機能f41が生成し、生成したマスター鍵とユーザIDを対応させてネットワーク鍵構成データベース24に登録する。

【0120】このユーザのマスター鍵は、ネットワーク通信管理用ワークステーション110のユーザ鍵管理データベース12に登録する必要があるが、この登録は、ネットワーク通信管理用ワークステーション110設置時、通信構成管理機能f15より直接入力しユーザ鍵管理データベース12に登録することもできるが、上記ネットワーク通信管理用ワークステーション110に割り当てたネットワークマスター鍵を使用し、スクランブル機能で暗号化して配送することもできる。同様に、ユーザのマスター鍵および、ネットワークマスター鍵の更新、削除に関するデータも上記ネットワーク通信管理用ワークステーション110に割り当てたネットワークマ

スター鍵を使用し、スクランブル機能で暗号化して、マスター鍵更新要求703として配送することもできる。

【0121】ネットワーク通信管理用ワークステーション110は、送付された鍵の登録、更新、削除に関するデータを復号化し、通信構成管理機能f15によりユーザ鍵管理データベース12の鍵の登録、更新、削除を実施する。

【0122】各ユーザへのマスター鍵の更新、および配布は、ネットワーク通信管理用ワークステーション110側でICカードまたはフロッピーディスクなどの記憶媒体に記録してオフラインで配布するか、変更前のユーザに割り当てられたマスター鍵で暗号化し、ネットワークを利用してオンラインで送付することができる。これらのうち、どちらの方式をとるかは、状況によって定めればよい。

【0123】次に、図8を参照して、否認防止部のソフト機能構成の実施例について説明する。

【0124】ユーザが他の相手ユーザにデータを送信する場合、ネットワーク通信管理部1020（図3参照）の実施例で説明したように、ユーザはパーソナルコンピュータなどの情報処理装置120（図4参照）のデータファイル処理機能f22（図4参照）にデータおよび宛先を入力するが、このユーザが送信するデータに対して否認防止の判定結果を必要とする場合は、更に、否認防止要求を入力する。

【0125】（1）ユーザが入力したデータはネットワーク通信管理部1020（図3参照）について説明したように、データファイル処理機能f22からネットワーク送受信管理機能f12に伝達されるが、「否認防止要求」はユーザセキュリティ機能f21を経由して通信管理セキュリティ機能f11に伝達される。通信管理セキュリティ機能f11では、否認防止要求801を受けてネットワーク送受信管理機能f12に伝達されたデータをもとに否認防止ファイル802を作成する。

【0126】否認防止ファイル802は、ユーザが入力したデータに識別子を付加したもの、または、ユーザが入力したデータをハッシュ関数で処理したハッシュ値に識別子を付加したものである。

【0127】ハッシュ関数は、「インターネットセキュリティ」オーム社、著者、佐々木良一、宝木和夫他のP91に記載されているように、

① 方向性 ; あるハッシュ関数の出力値が与えられた場合、同じ出力値をもたらす別のメッセージMを求めることが計算量的に困難であること。

【0128】② 衝突回避性 ; 同じハッシュ値となるような2つの異なるメッセージM1、M2を見つけることが、計算量的に困難であること。

【0129】の特性をもったものである。

【0130】（2）通信管理セキュリティ機能f11は、作成した否認防止ファイルを、鍵管理用ワークステ

ーション140の否認防止管理機能f41に送付し、否認防止管理機能f41は、送付された否認防止ファイル802を識別子と対応させて否認防止管理データベース26に格納する。

【0131】（3）ネットワーク送受信管理機能f12に伝達したデータは、暗号化通信処理部1030（図3参照）を介して送信先相手ユーザ側のネットワーク送受信管理機能f12に伝達される。復号化されたデータは、そのまま送信先相手ユーザに伝達されるが、否認防止要求801がある場合、通信セキュリティ管理機能f11は、送達されたデータをもとに、発信側と同様に、否認防止ファイル803を作成し、鍵管理用ワークステーション140の否認防止管理機能f41に伝達する。

【0132】否認防止管理機能f41は、受信側から送達された否認防止ファイル803を識別子と対応させて否認防止管理データベース26に格納する。

【0133】（4）否認防止管理機能f41は、送信側のユーザから送られた否認防止ファイル802と受信側のユーザから送られた否認防止ファイル803とを比較し、両者が一致する場合否認防止が正常と判定し、一致しない場合は異常と判定し、この否認防止判定結果を否認防止管理データベース26に登録する。

【0134】（5）データの送受信が終了後、送信側または受信側のユーザが否認防止照会要求をデータファイル処理機能f22に入力すると、この要求は、ユーザセキュリティ機能f21、通信管理セキュリティ機能f11を経由して否認防止管理機能f41に送達される。否認防止管理機能f41は否認防止照会要求を受けると、否認防止管理データベース26から否認防止判定結果を検索し、この結果を否認防止照会要求を入力したユーザに送付する。

【0135】（6）否認防止ファイルとして、ハッシュ値を作成する場合は、ハッシュ値のデータ量が小さいため、鍵管理用ワークステーション140の否認防止管理機能f41ばかりでなく、送信先相手のユーザに送信するデータに付加して送付することも可能である。

【0136】この場合、受信側の通信セキュリティ機能f11は、受信したデータをもとにハッシュ値を算出し、送信側のユーザが送付したハッシュ値と比較することにより、否認防止を確認することができる。

【0137】受信側の通信セキュリティ機能f11で実施した否認防止の確認結果が異常で、送信側と受信側のユーザ間でトラブルが生じた場合、第三者的な立場である鍵管理用ワークステーション140に問い合わせることにより、どちらに否があるか判定することが可能となる。

【0138】以下に、本発明を適用したネットワーク通信システムが提供する「鍵回復機能」の実施例について説明する。ここでは、暗号化通信を行う場合、図6に示すように、暗号に用いる鍵は二重の階層構造を有してい

るものとする。図6において、ユーザが送信するデータをMとし、ネットワーク通信管理用ワークステーション140が生成するスクランブル鍵 $K_s$ によりデータは暗号化され、暗号文 $E_{K_s}(M)$ が作成される。この暗号文を復号するためのデスクランブル鍵 $K_D$ を、鍵管理用ワークステーション140から送付されたセッション鍵 $P_1$ によって暗号化し、暗号文 $E_{P_1}(K_D)$ を作成している。

【0139】鍵回復機能は、暗号文 $E_{K_s}(M)$ に解説の情報に付加し、デスクランブル鍵 $K_D$ によらずに暗号文を解説する手段を与えるものである。

【0140】まず、図9を参照して、スクランブル鍵 $K_s$ でデータを暗号化の際、鍵回復機能を持たせるための付加データの作成手順について説明する。

【0141】(1)スクランブル鍵 $K_s$ を生成するとき、乱数を生成し $K_1$ 、 $K_2$ の排他的論理和(XOR、図では、直和記号で示している。)により、スクランブル鍵を $K_s = K_1 \text{ XOR } K_2$ と表現できるようにする。

【0142】(2) $P_1$ 、 $P_2$ を鍵回復用の鍵とし、ネットワーク通信管理用ワークステーション110(図4参照)および、鍵管理用ワークステーション140(図4参照)の鍵回復機能f43(図4参照)で保管するものとする。スクランブル鍵 $K_s$ を生成するときに生成した $K_1$ 、 $K_2$ をこの鍵回復用の鍵 $P_1$ 、 $P_2$ で暗号化して暗号文 $E_{P_1}(K_1)$ 、 $E_{P_2}(K_2)$ を作成する。このデータを、スクランブル鍵 $K_s$ で作成したデータの暗号文 $E_{K_s}(M)$ に付加するものとする。

【0143】次に、図10を参照して、この付加データで暗号文を復号する手順について説明する。

【0144】(1)暗号文から付加されたデータ $E_{P_1}(K_1)$ 、 $E_{P_2}(K_2)$ を分離し、鍵回復用の鍵 $P_1$ 、 $P_2$ で $K_1$ 、 $K_2$ を復号する。

【0145】(2) $K_1$ 、 $K_2$ の排他的論理和を取り、 $K_s = K_1 \text{ XOR } K_2$ として、スクランブル鍵 $K_s$ を生成する。共通鍵暗号の場合、スクランブル鍵 $K_s$ とデスクランブル鍵 $K_D$ とは同一であり、このスクランブル鍵 $K_s$ により、暗号文を復号することができる。

【0146】不測の事態が発生して、暗号文を解説する必要が生じた場合、暗号文を鍵管理用ワークステーション140(図4参照)に送付すれば、上記に示した手順により、鍵回復用の鍵 $P_1$ 、 $P_2$ を用いて暗号文を解説することができる。

【0147】以上で本ネットワーク通信システムを構成する6つの制御処理部のソフト機能の実施例について説明した。

【0148】本ネットワーク通信システムにおいて、アクセス管理部によるユーザ認証は、ネットワーク通信管理用ワークステーションにより、このワークステーションと接続するユーザに対して実施される。即ち、ユーザ

認証は複数のユーザで構成されるグループごとに実施される。また、ネットワーク通信管理部と暗号化通信処理部により、ネットワーク通信管理用ワークステーション間で暗号化通信が実施され、データを送信するユーザが暗号化し、これを受信するユーザが復号化するような、ユーザ対ユーザの暗号化通信は実施していない。

【0149】このため、図1に示すネットワーク通信システムにおいて、ネットワーク通信管理用ワークステーションと、これと接続する複数のユーザで構成されるグループにおいて、1つの閉じたネットワークを構築することができる。

【0150】次に、図11を参照して、1つのグループに設置されたネットワーク管理ワークステーションごとに共通鍵暗号方式で、閉じたネットワークを構築する場合の鍵の階層構造について説明する。ここでは、M個所のグループにネットワーク通信管理用ワークステーション110<1>～110<M>を設置している。

【0151】ネットワーク通信管理用ワークステーション110<j>(1≦j≦M)には、 $n_j$ 個のユーザが使用するパーソナルコンピュータなどの情報処理装置が接続しネットワークを構成している。ユーザには、ユーザID、および、マスター鍵としての秘密鍵が割り当てられている。これらのユーザをユーザ1～ユーザ $n_j$ とし、ユーザi(1≦i≦ $n_j$ )に割り当てられた秘密鍵を $P_{ji}$ 、ユーザIDを $ID_{ji}$ とする。ネットワーク通信管理ワークステーション110<j>は、このユーザ1～ユーザ $n_j$ のマスター鍵としての秘密鍵を管理するため、ユーザIDデータベース11に $n_j$ 個のユーザID{ $ID_{j1}$ ,  $ID_{j2}$ , ...,  $ID_{ji}$ , ...,  $ID_{jn_j}$ }を登録し、ユーザ鍵管理データベース12にユーザマスター鍵としての秘密鍵とユーザIDを対応させた $n_j$ 個のデータ( $ID_{j1}$ ,  $P_{j1}$ ), ( $ID_{j2}$ ,  $P_{j2}$ ), ..., ( $ID_{ji}$ ,  $P_{ji}$ ), ..., ( $ID_{jn_j}$ ,  $P_{jn_j}$ )を登録している。ユーザ認証は、ユーザに割り当てられたマスター鍵としての秘密鍵により、図4に示す共通鍵によるユーザ認証方式に従って実施される。

【0152】各ネットワーク通信管理用ワークステーション110<j>には、ネットワークIDとして $SD_j$ 、およびマスター鍵としての秘密鍵 $PS_j$ が割り当てられており、鍵管理用ワークステーション140がこれらのネットワークIDと秘密鍵 $SD_j$ を管理している。鍵管理用ワークステーション140のネットワークユーザIDデータベース25には、ネットワーク管理用ワークステーション110<j>のネットワークIDである $SD_j$ と、これが管理しているユーザのユーザID{ $ID_{j1}$ ,  $ID_{j2}$ , ...,  $ID_{jn_j}$ }を対応させて登録している。さらに、ネットワーク鍵構成データベース24には、ネットワークIDである $SD_j$ と秘密鍵 $PS_j$ を対応させて登録している。ネットワーク通信管理用ワークス



テーション110<j>に属するユーザiが暗号化通信を実施する場合、

(1) 送信先相手ユーザの宛先(名前)および送信するデータMを入力する。

【0153】(2) ネットワーク通信管理用ワークステーション110<j>は、鍵管理用ワークステーション140に暗号化通信を実施するためのセッション鍵発行の要求を行う。

【0154】(3) 鍵管理用ワークステーション140の鍵構成管理機能f41(図4参照)は、送信先相手ユーザの宛先(名前)をもとにネットワークユーザデータベース25を検索する。送信先相手ユーザがネットワーク通信管理用ワークステーション110<k>と接続するユーザであったとすると、相手ユーザのユーザIDであるID<sub>k1</sub>および、相手ユーザが接続するネットワーク通信管理用ワークステーション110<k>のネットワークIDであるSD<sub>k</sub>を取得する。

【0155】送信側ユーザが接続するネットワーク通信管理用ワークステーション110<j>のネットワークIDはSD<sub>j</sub>であり、相手先ユーザが接続するネットワーク通信管理用ワークステーション110<k>のネットワークIDはSD<sub>k</sub>である。

【0156】このネットワークIDであるSD<sub>j</sub>、SD<sub>k</sub>をキーとして、ネットワーク鍵構成データベース24を検索し、SD<sub>j</sub>とSD<sub>k</sub>とに対応する秘密鍵P<sub>sj</sub>、P<sub>sk</sub>を取得する。

【0157】次に、セッション鍵P<sub>T</sub>を生成し、取得した秘密鍵で暗号化し、暗号化セッション鍵E<sub>psj</sub>(P<sub>T</sub>)、E<sub>psk</sub>(P<sub>T</sub>)を作成する。

【0158】(4) 鍵管理用ワークステーション140は、暗号化セッション鍵E<sub>psj</sub>(P<sub>T</sub>)、E<sub>psk</sub>(P<sub>T</sub>)と、送信先相手ユーザが接続しているネットワーク管理用ワークステーション110<k>のネットワークIDであるSD<sub>k</sub>とをセッション鍵発行要求元のネットワーク通信管理用ワークステーション110<j>に発行する。

【0159】(5) ネットワーク通信管理用ワークステーション110<j>は、所有しているマスター鍵としての秘密鍵P<sub>Sj</sub>で暗号化セッション鍵E<sub>psj</sub>(P<sub>T</sub>)を復号し、セッション鍵P<sub>T</sub>を取得する。

【0160】次に、スクランブル鍵K<sub>s</sub>、デスクランブル鍵K<sub>d</sub>を生成し、まず送信するデータMを、スクランブル鍵K<sub>s</sub>で暗号化し、暗号文E<sub>ks</sub>(M)を作成する。次にデスクランブル鍵K<sub>d</sub>を、セッション鍵P<sub>T</sub>で暗号化し、暗号化デスクランブル鍵E<sub>pr</sub>(K<sub>d</sub>)を作成する。

【0161】一方、送付されたネットワークIDであるSD<sub>k</sub>により送信先相手をネットワーク通信管理用ワークステーション110<k>と指定して接続し、作成した暗号文E<sub>ks</sub>(M)、暗号化デスクランブル鍵E<sub>pr</sub>(K<sub>d</sub>)、および、送付された暗号化セッション鍵E

p<sub>k</sub>(P<sub>T</sub>)をデータとして合成して送付する。

【0162】(6) 上記暗号化されたデータを受信したネットワーク通信管理用ワークステーション110<k>は、所有しているマスター鍵としての秘密鍵P<sub>sk</sub>で暗号化セッション鍵E<sub>psk</sub>(P<sub>T</sub>)を復号し、セッション鍵P<sub>T</sub>を取得する。

【0163】次に、このセッション鍵より暗号化デスクランブル鍵E<sub>pr</sub>(K<sub>d</sub>)を復号し、デスクランブル鍵K<sub>d</sub>を取得する。このデスクランブル鍵K<sub>d</sub>により暗号文E<sub>ks</sub>(M)を復号し、データMを取り出す。この復号して得られたデータMを送信先相手のユーザIDがID<sub>k1</sub>であるユーザに送付する。

【0164】以上の手順で、ネットワーク管理用ワークステーション110<j>に接続するユーザID<sub>ji</sub>から、ネットワーク管理用ワークステーション110<k>に接続するユーザID<sub>k1</sub>に暗号化通信が実施される。

【0165】本ネットワーク通信システムの鍵管理用ワークステーションは、各ネットワーク通信管理用ワークステーションに割り付けられたマスター鍵としての秘密鍵の管理は実施するものの、各ネットワーク通信管理用ワークステーションに接続するユーザに対しては、割り当てられたユーザIDは管理するものの、割り当てられたマスター鍵としての秘密鍵は管理していない。

【0166】逆に、ユーザに対して割り当てられたマスター鍵としての秘密鍵を管理しているのは、このユーザと接続しているネットワーク通信管理用ワークステーションだけである。

【0167】このことから、ネットワーク通信管理用ワークステーションと、これと接続しているユーザ間で一つのグループとして閉じたネットワークを構築していることがわかる。

【0168】共通鍵暗号でシステムを構築する場合、各ユーザに割り当てられたマスター鍵としての秘密鍵は、ユーザ認証のみに用いられ、ネットワーク外部へは、暗号化通信に用いる鍵として使用されないため、このネットワーク通信管理用ワークステーションが設置されているグループは、ユーザ認証用として独自の暗号アルゴリズムを使用してもよい。

【0169】セキュリティを確保するため、このグループのネットワーク内ユーザ間相互の暗号化通信を、ユーザに割り当てられたマスター鍵を使用して実施することも可能である。

【0170】実施例として、ネットワーク管理用ワークステーションに属するユーザIDがID<sub>ji</sub>であるユーザからユーザIDがID<sub>jr</sub>であるユーザに暗号化通信を実施するものとする、ネットワーク通信管理用ワークステーションは、セッション鍵Tを生成し、ID<sub>ji</sub>に対応するマスター鍵としての秘密鍵P<sub>i</sub>とID<sub>jr</sub>に対応するマスター鍵としての秘密鍵P<sub>r</sub>でセッション鍵



$P_T$ を暗号化し、暗号化セッション鍵 $E_{P_i}(T)$ 、 $E_{P_r}(T)$ を生成する。これをユーザIDがID $j_i$ であるユーザに送付する。

【0171】送信元のユーザは、マスター鍵としての秘密鍵 $P_i$ で暗号化セッション鍵 $E_{P_j}(T)$ を復号し、セッション鍵 $P_r$ を取得する。

【0172】このセッション鍵 $P_r$ によりデータ $M$ を暗号化し、暗号文 $E_r(M)$ を作成し、送付された暗号化セッション鍵 $E_{P_r}(T)$ をこの暗号文に付加して送信する。この暗号文 $E_r(M)$ と暗号化セッション鍵 $E_{P_r}(T)$ を送付することで、ネットワーク内で暗号化通信を実施することが可能となる。

【0173】この場合、グループに設置されたネットワーク通信管理用ワークステーションは、通信セキュリティ管理機能において、グループのネットワーク内の暗号化通信に使用するセッション鍵を生成することになる。

【0174】以上で、本発明のネットワーク通信システムを構成する6つの制御処理部のソフト機能の実施例を示した。図4に示すネットワーク通信システムに組み込まれるソフト機能において、暗号演算に関する処理は、ユーザセキュリティ機能、通信管理セキュリティ機能、スクランブル機能、デスクランブル機能で実施している。

【0175】つぎに、図12を参照して、このような暗号演算を実施する暗号処理装置をユーザが使用するパーソナルコンピュータなどの情報処理装置、およびネットワーク通信管理用ワークステーションに組み込んだ実施例について説明する。

【0176】ユーザが使用するパーソナルコンピュータ121は、ユーザが使用する情報処理装置の1つであり、ユーザが使用するCAD122(図2参照)でもよい。ユーザが使用するパーソナルコンピュータ121は、通常、CPU2およびデータ処理装置3を内蔵しており、データファイル処理機能f22(図4参照)、ユーザセキュリティ機能f21(図4参照)に関する処理を行う。ネットワーク通信管理用ワークステーション4も、CPU5およびデータ処理装置6を内蔵しており、ネットワーク送受信管理機能f12(図4参照)、通信セキュリティ管理機能f11(図4参照)、通信構成管理機能f15(図4参照)、スクランブル機能f13(図4参照)、デスクランブル機能f14(図4参照)に関する処理を行う。

【0177】ユーザセキュリティ機能f21(図4参照)、および、通信管理セキュリティ機能f11(図4参照)によりアクセス管理部1010(図3参照)が行うユーザ認証のための暗号処理を、ユーザ認証用暗号装置7、8により実施している。

【0178】ユーザ認証の過程で、ユーザは自分に割り当てられたマスター鍵を入力する。このマスター鍵はユーザが暗記して入力することも可能であるが、本実施例

では、ICカードにマスター鍵を記録させておきICカード制御部9から入力している。

【0179】ユーザが使用するパーソナルコンピュータ121とネットワーク管理用ワークステーション110とはLAN10で接続されており、ネットワーク11を構成している。ネットワーク管理用ワークステーション110と接続するユーザに割り当てられたマスター鍵は、ユーザ鍵管理データベース12に登録され、ICカードで入力されるユーザのマスター鍵を使用して暗号化通信を行い、ユーザ認証が行われる。

【0180】ネットワーク通信管理用ワークステーション110と、これに属するユーザとはLAN10で接続され、接続する全てのユーザに対して、このネットワーク通信管理用ワークステーションワークステーション110によるユーザ認証が実施される。このため、このグループで独立の閉じたネットワークを構成することができる。

【0181】アクセス管理部1010(図3参照)によるユーザ認証が終了すると、ネットワーク通信管理用ワークステーション110間で暗号化通信処理部1030(図3参照)による暗号化通信が実施される。暗号化通信処理部1030(図3参照)により暗号化通信を行う場合、鍵管理用ワークステーション140(図4参照)から暗号化されたセッション鍵が送付される。ここでネットワーク通信管理ワークステーション110と接続するユーザ間で閉じたネットワークを構成するため、図11の共通鍵暗号方式の鍵の階層構造で示すように、ネットワーク通信管理用ワークステーション110には、ネットワークマスター鍵を割り当てておくものとする。これより、送信側のネットワーク通信管理用ワークステーション110のネットワークマスター鍵を $P_{si}$ 、受信側のネットワーク通信管理用ワークステーション110のネットワークマスター鍵を $P_{sj}$ とすると、鍵管理用ワークステーション140(図4参照)は、セッション鍵 $P_r$ を生成し、これを上記ネットワークマスター鍵 $P_{si}$ 、 $P_{sj}$ で暗号化し、暗号文 $E_{P_{si}}(P_r)$ 、 $E_{P_{sj}}(P_r)$ を送信する。

【0182】図4に示すネットワーク通信システムに組み込むソフト機能のうち、まずスクランブル機能について説明する。

【0183】図12のセッション鍵復号化装置13は、鍵管理用ワークステーションが送付した暗号化セッション鍵 $E_{P_{si}}(P_r)$ を送受信設備14を経由して受信する。これをネットワーク通信管理用ワークステーション110に割り当てられ、ユーザ鍵管理データベース12に格納しているネットワークマスター鍵 $P_{si}$ で復号演算を行い、セッション鍵 $P_r$ を取得し、スクランブル鍵暗号化装置15に引き渡す。スクランブル鍵、デスクランブル鍵生成装置16は、データの暗号化に使用するスクランブル鍵 $K_s$ および、データの復号化に使用するデス

スクランブル鍵 $K_D$ を生成し、暗号処理管理装置17に引き渡す。暗号処理管理装置17は、スクランブル鍵 $K_S$ をデータ暗号化装置18に引き渡し、デスクランブル鍵 $K_D$ をデスクランブル鍵暗号化装置15に引き渡す。ユーザが入力したデータ $M$ は、ユーザが使用するパーソナルコンピュータ1のデータ処理装置3より入力され、データ暗号化装置18へ伝達される。デスクランブル鍵暗号化装置15は、セッション鍵復号化装置13より送られたセッション鍵 $P_T$ によりデスクランブル鍵 $K_D$ の暗号化を行い暗号文 $E_{PT}(K_D)$ を作成し、データ暗号化装置18は、スクランブル鍵 $K_S$ によりデータ $M$ の暗号化を行い暗号文 $E_{KS}(M)$ を作成する。この暗号化の過程を暗号化処理管理装置17が管理している。データの暗号化通信を実施する場合、データの暗号文 $E_{KS}(M)$ と暗号化デスクランブル鍵 $E_{PT}(K_D)$ を同時に受信しても、まず、 $K_D$ を復号化してからでないと $E_{KS}(M)$ を復号化することができない。このように、暗号化デスクランブル鍵 $E_{PT}(K_D)$ は、暗号文 $E_{KS}(M)$ よりも先に受信し復号しておく必要がある。

【0184】次に、図13を参照して、共通鍵暗号でのスクランブル鍵の切り替えに、データの復号を円滑にするためのデスクランブル鍵配送シーケンスについて説明する。

【0185】ユーザAからユーザBに暗号化通信を実施する場合、ある定まったデータ量が伝達されると、暗号化に使用するスクランブル鍵を新しく生成してスクランブル鍵の切り替えを実施し、暗号化通信のセキュリティを確保するようにしている。図13は、このスクランブル鍵の切り替えとデータの暗号化のシーケンスを示している。スクランブル鍵の $i-1$ 回目の切り替え時のデータを $M_{i-1}$ 、 $i$ 回目の切り替え時のデータを $M_i$ 、 $i+1$ 回目の切り替え時のデータを $M_{i+1}$ とする。

【0186】(S1301) データ $M_{i-1}$ を暗号化する場合、スクランブル鍵とデスクランブル鍵の生成を行うが、このときデータ $M_i$ を暗号化する時に使用するスクランブル鍵 $K_{Si}$ とデスクランブル鍵 $K_{Di}$ を生成し、一旦メモリに格納しておく。

【0187】(S1302) スクリンブル鍵を切り替え、データ $M_i$ を暗号化する場合、データ $M_{i+1}$ を暗号化する時に使用するスクランブル鍵 $K_{Si+1}$ とデスクランブル鍵 $K_{Di+1}$ を生成し、一旦メモリに格納する。このメモリからデスクランブル鍵 $K_{Di}$ 、 $K_{Di+1}$ を取り出し、セッション鍵 $P_T$ により暗号化し、暗号文 $E_{PT}(K_{Di}$ 、 $K_{Di+1})$ を作成する。同様にメモリからスクランブル鍵 $K_{Si}$ を取り出し、データ $M_i$ を暗号化し暗号文 $E_{KS_i}(M_i)$ を作成する。次に、作成した暗号文 $E_{PT}(K_{Di}$ 、 $K_{Di+1})$ 、 $E_{KS_i}(M_i)$ をペアとしてユーザBに送付する。

【0188】暗号文を送付後、使用したスクランブル鍵 $K_{Si}$ とデスクランブル鍵 $K_{Di}$ をメモリから消去する。

【0189】ユーザBはセッション鍵 $P_T$ により送付された暗号文 $E_{PT}(K_{Di}$ 、 $K_{Di+1})$ を復号化し、デスクランブル鍵 $K_{Di}$ 、 $K_{Di+1}$ を取り出す。取り出したデスクランブル鍵 $K_{Di+1}$ を、メモリに格納し次に送付される暗号文を復号する準備をする。

【0190】(S1303) スクリンブル鍵を切り替え、データ $M_{i+1}$ を暗号化する場合、データ $M_{i+2}$ を暗号化する時に使用するスクランブル鍵 $K_{Si+2}$ とデスクランブル鍵 $K_{Di+2}$ を生成し、一旦メモリに格納する。このメモリからデスクランブル鍵 $K_{Di+1}$ 、 $K_{Di+2}$ を取り出し、セッション鍵 $P_T$ により暗号化し、暗号文 $E_{PT}(K_{Di+1}$ 、 $K_{Di+2})$ を作成する。同様にメモリからスクランブル鍵 $K_{Si+1}$ を取り出し、データ $M_{i+1}$ を暗号化し暗号文 $E_{KS_{i+1}}(M_{i+1})$ を作成する。次に、作成した暗号文 $E_{PT}(K_{Di+1}$ 、 $K_{Di+2})$ 、 $E_{KS_{i+1}}(M_{i+1})$ をペアとしてユーザBに送付する。

【0191】(4) 暗号文を送付されたユーザBは、準備していたデスクランブル鍵 $K_{Di+1}$ により暗号文 $E_{KS_{i+1}}(M_{i+1})$ を復号化し、データ $M_{i+1}$ を取得する。データ $M_{i+1}$ を取得後使用したデスクランブル鍵 $K_{Di+1}$ をメモリから消去する。

【0192】次に、セッション鍵 $P_T$ により送付された暗号文 $E_{PT}(K_{Di+1}$ 、 $K_{Di+2})$ を復号化し、デスクランブル鍵 $K_{Di+1}$ 、 $K_{Di+2}$ を取り出す。取り出したデスクランブル鍵 $K_{Di+2}$ をメモリに格納し次に送付される暗号文を復号する準備をする。

【0193】前述のデータ $M_{i+1}$ の復号化がうまく行かなかった場合、取り出したデスクランブル鍵 $K_{Di+1}$ を再度復号化演算を試みるものとする。前述のデータ $M_{i+1}$ の復号化がうまく行っている時は、デスクランブル鍵 $K_{Di+1}$ は消去するものとする。

【0194】以上のようなシーケンスにより、データの暗号文の送付と同時にデータの復号が可能となる。暗号処理管理装置17(図12参照)は、上記シーケンスでデスクランブル鍵の暗号文 $E_{PT}(K_{Di}$ 、 $K_{Di+1})$ および、データ $M_i$ の暗号文 $E_{KS_i}(M_i)$ が作成されるように管理している。これらの暗号文が作成されると合成装置19(図12参照)に送付され、暗号文をデータファイルとして合成し、送受信設備14(図12参照)を経由して配信される。

【0195】鍵管理用ワークステーションからは、相手先に送付するセッション鍵に関する暗号文 $E_{PS_j}(P_T)$ が送られてくるが、この暗号文はそのまま合成装置19(図12参照)、送受信設備14(図12参照)を経由して相手先に配信される。

【0196】次に、図12を参照して、ネットワーク通信システムのソフト機能(図4参照)のうちのデスクランブル機能について説明する。

【0197】(1) セッション鍵復号化装置13は、送信側のネットワーク通信管理用ワークステーションが送

付した暗号化セッション鍵 $E_{P_{Sj}}(P_T)$ を送受信設備14を経由して受信する。これをネットワーク通信管理用ワークステーション110に割り当てられたネットワークマスター鍵 $P_{Sj}$ で復号化を行い、セッション鍵 $P_T$ を取得し、デスクランブル鍵復号装置20に引き渡す。

【0198】(2) 受信する暗号文のデータはスクランブル機能で示したように、デスクランブル鍵についての暗号文 $E_{P_T}(K_{Di}, K_{Di+1})$ とデータ $M_i$ についての暗号文 $E_{K_{Si}}(M_i)$ とで構成されている。このデータは送受信設備14を経由して分配装置21に送達される。

【0199】ここで暗号化デスクランブル鍵 $E_{P_T}(K_{Di}, K_{Di+1})$ とデータの暗号文 $E_{K_{Si}}(M_i)$ に分離し、デスクランブル鍵同期装置22に引き渡され、暗号化デスクランブル鍵は、デスクランブル鍵復号化装置20へ、データの暗号文はデータ復号化装置23に引き渡される。

【0200】(3) デスクランブル鍵復号化装置20は、セッション鍵復号化装置13からセッション鍵 $P_T$ が送付されており、このセッション鍵 $P_T$ を用いて、デスクランブル鍵同期装置22から送付された暗号化デスクランブル鍵 $E_{P_T}(K_{Di}, K_{Di+1})$ の復号化し、デスクランブル鍵 $K_{Di}, K_{Di+1}$ を取得する。デスクランブル鍵同期装置22は、図13に示すデスクランブル鍵の配送シーケンスに従ってデスクランブル鍵をデータ復号化装置23に引き渡す。データ復号化装置23は、送付されたデスクランブル鍵 $K_{Di}$ で送付された暗号文 $E_{K_{Si}}(M_i)$ を復号し、データ $M_i$ を取得する。取得したデータ $M_i$ は、送信先相手ユーザの使用するパーソナルコンピュータ1のデータ処理装置3に送付される。

【0201】以上本発明のネットワーク通信システムを構成する6つの制御処理部について、共通鍵暗号を用いた場合のソフト機能構成の実施例について示した。

【0202】次に、図14を参照して、公開鍵暗号を用いた場合のソフト機能構成の実施例について説明する。図14は、公開鍵暗号を用いた場合のアクセス管理部のソフト機能構成が示されている。

【0203】公開鍵暗号アルゴリズムとしては、信学技報 TECHNICAL REPORT OF IEICE ISEC97-15 (1997-07)「楕円曲線を利用した高速暗号化法」 宝木和夫、車谷博之に記載された楕円曲線暗号を用いるものとし、この楕円曲線暗号の鍵の演算を記載するために必要な楕円曲線のベースポイントを $P$ とする。

【0204】パーソナルコンピュータなどの情報処理装置を使用する各ユーザには、鍵管理局よりユーザID、マスター鍵としての秘密鍵 $d_{ID}$ および対応する公開鍵 $Q_{ID}(=d_{ID} \cdot P; \cdot$ は、楕円曲線上の演算)が割り当てられている。

【0205】ネットワーク通信管理用ワークステーションのユーザIDデータベースには、このワークステー

ションに接続しているユーザに割り当てられたユーザIDが登録され、ユーザ鍵管理データベースには、このワークステーションに接続しているユーザの公開鍵がユーザIDと対応させて登録されている。

【0206】アクセス管理部では、ユーザが使用するパーソナルコンピュータなどの情報処理装置のユーザセキュリティ機能とネットワーク通信管理用ワークステーションの通信セキュリティ機能間の暗号化通信によって、ユーザ認証を実施する。以下、この実施例を示す。

【0207】(1) ユーザが、本ネットワーク通信システムを利用する場合、ユーザが使用するパーソナルコンピュータなどの情報処理装置にアクセス要求を入力する。ユーザセキュリティ機能は、「シーケンス番号」を付加しユーザ認証要求として通信セキュリティ機能に送付する。

【0208】(2) この要求を受けて、通信セキュリティ機能はユーザに割り当てられた「ユーザID」をキーとして、ユーザIDデータベースを検索し、「ユーザID」が該当すれば、時刻情報(「月」, 「日」, 「時」, 「分」, 「秒」)と乱数から構成されるチャレンジコードCACを生成し、ユーザセキュリティ機能に送付する。

【0209】(3) ユーザは、フロッピーディスクまたは、ICカードにユーザに割り当てられたマスター鍵としての秘密鍵 $d_{ID}$ を保管しており、この電子媒体に記録されている鍵を入力する。このマスター鍵で送付されたチャレンジコードCACに署名作成演算を実施し、作成した署名データ $Sd_{ID}(CAC)$ を通信セキュリティ機能に送付する。

【0210】(4) 通信管理セキュリティ機能は、「ユーザID」をキーとしてユーザ鍵管理データベースを検索し、ユーザに割り当てられているマスター鍵としての秘密鍵 $d_{ID}$ に対応する公開鍵 $Q_{ID}$ を取り出し、送付された署名データ $Sd_{ID}(CAC)$ と生成したチャレンジコードCACをもとに署名検証演算を実施する。

【0211】署名検証演算により、ユーザセキュリティ機能で使用した秘密鍵 $d_{ID}$ と通信管理セキュリティ機能で使用した公開鍵 $Q_{ID}$ が楕円曲線上の演算( $Q_{ID}=d_{ID} \cdot P; \cdot$ は楕円曲線上の演算)として対応し、かつ、チャレンジコードCACが通信経路の途中で改竄されなければ、ユーザを正当なユーザと判断することができ、認証判定結果を認証完了とする。逆に、上記暗号処理に使用する鍵が対応しなかったり、チャレンジコードCACが改竄された場合は、認証判定結果を認証エラーとする。そして、このようにして得られた認証判定結果をユーザセキュリティ機能に返送する。

【0212】(5) ユーザセキュリティ機能は、認証判定結果がユーザ認証完了の場合、「シーケンス番号」を除いてユーザ認証結果としネットワーク通信管理部に伝達する。

【0213】なお、図3におけるネットワーク通信管理部のソフト機能構成は、暗号アルゴリズムとして、共通鍵暗号、公開鍵暗号のどちらを使用した場合も同じである。

【0214】次に、図15を参照して、公開鍵暗号アルゴリズムを使用した場合の暗号化通信処理部のソフト機能構成の実施例について説明する。

【0215】公開鍵暗号アルゴリズムとしては、アクセス管理部1010（図3参照）で用いた公開鍵暗号アルゴリズムと同様、楕円曲線暗号アルゴリズムを使用しており、鍵の演算に必要な楕円曲線のベースポイントをPとしている。

【0216】暗号化通信を実施する場合、ネットワーク通信管理用ワークステーション110のスクランブル機能f13は、ネットワーク送受信管理機能f12（図4参照）から送信されるデータを受け取る。

【0217】次に、鍵管理用ワークステーション140の鍵構成管理機能f41からセッション鍵の発行を受け、この鍵をもとに受け取ったデータを暗号化し暗号文を作成し、送信先相手ユーザ側のネットワーク通信管理用ワークステーション110のデスクランブル機能f14に送信する。

【0218】デスクランブル機能f14は、送付された暗号文を復号化し、データを取得する。

【0219】暗号化通信処理部1030（図3参照）を運用する前提条件として、前述のアクセス管理部1010（図3参照）と同様、パーソナルコンピュータなどの情報処理装置を使用する各ユーザには、鍵管理局より、ユーザIDとマスター鍵として、秘密鍵 $d_{ID}$ と、この秘密鍵に対応する公開鍵 $Q_{ID}$ （ $=P \cdot d_{ID}$ ； $\cdot$ は楕円曲線上の演算）とを割り当てられており、鍵管理用ワークステーション140のネットワーク鍵構成データベース24に、ユーザに割り当てた公開鍵 $Q_{ID}$ をユーザIDと対応させて登録し管理している。同様にネットワーク通信管理用ワークステーション110には、このワークステーションと接続するすべてのユーザの公開鍵 $Q_{ID}$ をユーザIDと対応させて、ユーザ鍵管理データベース12に登録し管理しているものとする。

【0220】以下、この暗号化通信処理部の実施例を示す。

【0221】（1）暗号化通信を実施する場合、暗号化通信要求が発生すると、鍵管理用ワークステーション140は、ネットワーク鍵構成データベース24を検索し、ユーザの送信する相手先ユーザの公開鍵 $Q_{YID}$ を取得する。この公開鍵 $Q_{YID}$ をセッション鍵として発信側のユーザの接続するネットワーク通信管理用ワークステーション110に送付する。

【0222】（2）発信側のユーザの接続するネットワーク通信管理用ワークステーション110では、送信するデータM1504を、ネットワーク送受信管理機能f

12から受け取り、暗号化するためのスクランブル鍵 $K_s$ 1501と復号するためのデスクランブル鍵 $K_D$ 1502を生成する。このスクランブル鍵 $K_s$ 1501とデスクランブル鍵 $K_D$ 1502とを運用する暗号アルゴリズムは共通鍵暗号アルゴリズムとする。

【0223】次に、ユーザの入力するデータM1504をスクランブル鍵 $K_s$ 1501で暗号化し、暗号文 $E_{KS}$ （M）1506を作成する。

【0224】また、デスクランブル鍵 $K_D$ 1502を送付されたセッション鍵としての公開鍵 $Q_{YID}$ 1507で暗号化し、暗号化デスクランブル鍵 $E_{Q_{YID}}(K_D)$ 1508を生成する。

【0225】公開鍵暗号の場合、送付された鍵 $Q_{YID}$ 1508はそのまま暗号化のための鍵として使用することができる。

【0226】このようにして作成した2組の暗号文 $E_{KS}$ （M）1506と $E_{Q_{YID}}(K_D)$ 1508とを送信相手先のユーザが接続するネットワーク通信管理用ワークステーション110に送信する。

【0227】（3）送信相手先のネットワーク通信管理用ワークステーション110は、ユーザ鍵管理データベース12を検索し、管理しているユーザのマスター鍵としての秘密鍵 $D_{YID}$ 1510を取得する。

【0228】この取得した秘密鍵 $D_{YID}$ 1510で、暗号化デスクランブル鍵 $E_{Q_{YID}}(K_D)$ 1508を復号し、デスクランブル鍵 $K_D$ 1503を取得する。次に、このデスクランブル鍵 $K_D$ 1503を用いて、暗号文 $E_{KS}$ （M）1506を復号し、データM1505を得る。

【0229】（4）取得したデータM1505は、ネットワーク送受信管理機能f12を経由して送信先相手ユーザに伝達される。

【0230】以上の方式で、ユーザからユーザへの暗号化通信を実施する。

【0231】スクランブル鍵 $K_s$ 、デスクランブル鍵 $K_D$ を運用する共通鍵暗号アルゴリズムとしてCSデジタル放送で実績のあるMULTI2暗号アルゴリズムを用いる。

【0232】マスター鍵、セッション鍵を運用する暗号アルゴリズムは、前述のように共通鍵暗号アルゴリズムとは異なる楕円曲線暗号アルゴリズムを用いており、これにより、二重暗号方式が構成され、セキュリティの向上が図られている。

【0233】次に、本発明のネットワーク通信システムにおいて、公開鍵暗号として楕円曲線暗号を用いた場合の鍵管理部の実施例を示す。公開鍵暗号を用いた場合の鍵管理部のソフト機能は、図7に示す共通鍵暗号の場合のソフト機能と同じである。前述の公開鍵暗号アルゴリズムを使用した場合の暗号化処理部、およびアクセス管理部のソフト機能構成の実施例に示すように、各ユーザのマスター鍵は秘密鍵 $d_{ID}$ であり、この秘密鍵と楕円曲

線上の演算で公開鍵 $Q_{ID}$  ( $= d_{ID} \cdot P$ ;  $\cdot$ は楕円曲線上の演算)が対応している。

【0234】また、スクランブル鍵およびデスクランブル鍵の暗号アルゴリズムは、共通鍵暗号アルゴリズムとしてMULTI2暗号アルゴリズムとしている。

【0235】鍵管理部は、本ネットワーク通信システムを使用するすべてのユーザのマスター鍵に関する情報および、暗号化通信に関与するセッション鍵を管理している。

【0236】以下、図7を参照して、この鍵管理部について説明する。

【0237】(1) マスター鍵の管理

本ネットワーク通信システムを使用する全ユーザには、ユーザIDおよびこれと対応してマスター鍵としての秘密鍵 $d_{ID}$ および対応する公開鍵 $Q_{ID}$ が割り当てられており、同様にネットワーク通信管理用ワークステーション110には、ネットワークIDおよびこれと対応して、マスター鍵としての秘密鍵 $D_s$ 、対応する公開鍵 $Q_s$ が割り当てられている。

【0238】鍵管理用ワークステーション140のネットワーク鍵構成データベース24には、全ユーザに上記ユーザIDと、このユーザに割り当てられた公開鍵とを対応させ、また、全ネットワーク通信管理用ワークステーション110に上記ネットワークIDと、このワークステーションに割り当てられた公開鍵とを対応させて登録している。

【0239】同じようにして、ネットワーク通信管理用ワークステーション110のユーザ鍵管理データベース12には、このワークステーション110に割り当てられた上記ネットワークIDと対応して、マスター鍵としての秘密鍵 $D_s$ 、対応する公開鍵 $Q_s$ とを登録するとともに、このワークステーション110と接続するすべてのユーザのユーザIDとマスター鍵である秘密鍵 $d_{ID}$ および対となる公開鍵である $Q_{ID}$ とを対応して登録している。公開鍵暗号を用いる場合、ネットワーク鍵構成データベース24は、公開鍵のみを登録し、秘密鍵を登録する必要がない。

【0240】上記ユーザのマスター鍵としての秘密鍵および対となる公開鍵は、ネットワーク通信管理用ワークステーション110の通信構成管理機能f15と、鍵管理用ワークステーション140の鍵構成管理機能f41とによって管理されており、このユーザのマスター鍵の登録、更新、削除はこれらの機能のより実施される。

【0241】ネットワーク通信管理用ワークステーション110設置時に、このワークステーション110のネットワークIDと、秘密鍵および対応する公開鍵を鍵管理用ワークステーション140の鍵構成管理機能f41が生成し、ネットワークIDデータベース27およびネットワーク鍵構成データベース24に登録するとともに、ネットワーク通信管理用ワークステーション110

の通信構成管理機能f15により、ユーザIDデータベース28およびユーザ鍵管理データベース12に登録する。

【0242】各ユーザの秘密鍵および対となる公開鍵も、鍵構成管理機能f41が生成し、公開鍵とユーザIDとを対応させてネットワーク鍵構成データベース24に登録する。生成した各ユーザの秘密鍵および対となる公開鍵は、ユーザ鍵管理データベース12に登録する必要があるが、上記ネットワーク通信管理用ワークステーション110設置時、通信構成管理機能f15より直接入力し登録することもできるが、ネットワーク通信用ワークステーション110に割り当てられた公開鍵を使用し、スクランブル機能f14により暗号化して配送することも可能である。

【0243】同様に、ユーザのマスター鍵および、ネットワーク通信管理用ワークステーション110のマスター鍵の更新、削除に関するデータも上記ネットワーク通信管理用ワークステーション110に割り当てた公開鍵を使用し、スクランブル機能f14で暗号化して配送することもできる。

【0244】鍵情報は、本ネットワーク通信システムにおいて、暗号化通信の根幹となる情報であるため、その正当性をネットワーク通信管理用ワークステーション110で確認する必要がある。このため、鍵管理用ワークステーション140には、固有のマスター鍵である秘密鍵 $d_c$ および対応する公開鍵である $Q_c$  ( $= d_c \cdot P$ )を定め、送付する鍵情報に、鍵管理用ワークステーションによる署名作成演算(電子署名)を実施する。

【0245】当然、この公開鍵は、ネットワーク通信管理用ワークステーション110へ公開しておく。

【0246】次に、上記マスター鍵の管理の手順について説明する。鍵構成管理機能140の生成するユーザの鍵に関する情報をMとする。ここでは、鍵を更新する場合について示す。

【0247】(i) Mは、更新するユーザのユーザID、更新する秘密鍵 $d_{ID}$ 、公開鍵 $Q_{ID}$ および更新日時で構成される。

【0248】全てのネットワーク構成管理データベース24を検索し、得られたユーザと接続するネットワーク通信管理用ワークステーション110のネットワークIDを $I_s$ 、公開鍵 $Q_s$ とする。この公開鍵 $Q_s$ には、鍵管理用ワークステーション40による署名作成演算を実行して配布し、使用する側は署名検証演算により公開鍵 $Q_s$ の正当性を確認するものとする。

【0249】鍵情報を暗号化するためスクランブル機能が生成したスクランブル鍵を $K_s$ 、デスクランブル鍵を $K_D$ とする。

【0250】(ii) 鍵情報Mをスクランブル鍵 $K_s$ で暗号化し、暗号文 $E_{K_s}(M)$ を作成する。

【0251】デスクランブル鍵 $K_D$ を公開鍵 $Q_s$ で暗号化

し、暗号化デスクランブル鍵 $E_{qs}(K_D)$ を作成する。

【0252】また、鍵情報Mに対して、鍵管理用ワークステーション140のマスター鍵である秘密鍵 $d_c$ で署名作成演算を実施し署名データ $S_{dc}(M)$ を作成する。

【0253】次に、この $E_{ks}(M)$ 、 $E_{qs}(KD)$ 、 $S_{dc}(M)$ をネットワークIDである $I_s$ で宛先を指定し、送信する。

【0254】(iii)受信側のネットワーク管理用ワークステーション110は、デスクランブル機能f14に $E_{ks}(M)$ 、 $E_{qs}(KD)$ 、 $S_{dc}(M)$ を送付する。デスクランブル機能f14は、ネットワーク通信管理用ワークステーション110に割り当てられた秘密鍵 $d_s$ により $E_{qs}(K_D)$ を復号し、デスクランブル鍵 $K_D$ を取得する。

【0255】次に、 $K_D$ により $E_{ks}(M)$ を復号し、鍵に関する情報Mを取得する。

【0256】(iv)鍵に関する情報M、と鍵管理用ワークステーション140の公開鍵 $Q_c$ を用いて署名データ $S_{dc}(M)$ に対し署名検証演算を実施し、鍵に関する情報Mが正当な鍵管理用ワークステーション140から送付されたものであることを確認する。

【0257】この確認が得られたら鍵情報Mを、通信構成管理機能f15に送り、この鍵情報Mをもとにユーザ鍵管理データベース12を更新する。

【0258】(v)各ユーザへのマスター鍵の更新、および配布は、ネットワーク通信管理用ワークステーション110側でICカードまたはフロッピーディスクなどの記録媒体に記録してオフラインで配布するか、変更前のユーザに割り当てられた公開鍵で暗号化し、ネットワークを利用してオンラインで送付することができる。これらのうち、どちらの方式をとるかは、状況によって定める。

【0259】(2)セッション鍵の管理

(i)暗号化通信処理部1030(図3参照)で暗号化通信を行う場合、発信側ユーザのネットワーク通信管理用ワークステーション110の通信セキュリティ管理機能f11から、発信側のユーザIDと送信先相手のユーザIDを付加したセッション鍵発行要求が、鍵管理ワークステーション140の鍵構成管理機能f41に送付される。

【0260】(ii)鍵構成管理機能f41は、ユーザIDをキーとしてネットワーク鍵構成データベース24を検索し、送信先相手ユーザのマスター鍵に対応する公開鍵 $Q_{YID}$ を取り出す。

【0261】取り出した公開鍵 $Q_{YID}$ に対して、鍵管理用ワークステーション140のマスター鍵である秘密鍵 $d_c$ で署名作成演算を実施し署名データ $S_{dc}(Q_{YID})$ を作成する。

【0262】この公開鍵 $Q_{YID}$ と署名データ $S_{dc}(Q_{YID})$ とを、発信側ユーザのネットワーク通信管

理用ワークステーション110の通信セキュリティ管理機能f11に発行する。

【0263】(iii)公開鍵 $Q_{YID}$ と署名データ $S_{dc}(Q_{YID})$ とを受信した通信セキュリティ管理機能f11は、鍵管理用ワークステーション140の公開鍵 $Q_c$ を用いて署名データ $S_{dc}(Q_{YID})$ に対し署名検証演算を実施し、公開鍵 $Q_{YID}$ が正当な鍵管理用ワークステーション140から送付されたものであることを確認する。

【0264】公開鍵 $Q_{YID}$ は、セッション鍵として、デスクランブル鍵を暗号化するために使用する。

【0265】このようにして、セッション鍵が発行される。

【0266】次に、本発明のネットワーク通信システムにおいて、公開鍵暗号として楕円曲線暗号を用いた場合の否認防止部のソフト機能について説明する。

【0267】公開鍵暗号を用いた場合の否認防止部のソフト機能は、図8に示される、共通鍵暗号を用いた場合のソフト機能と同じであり、共通鍵暗号と同様、ユーザが否認防止要求を入力した場合、ネットワーク通信管理用ワークステーションの通信管理セキュリティ機能において、送信するデータをもとに否認防止ファイルの作成を行う。

【0268】公開鍵暗号の場合、この否認防止ファイルは送信するデータに署名作成演算を実施したものを用い、鍵管理ワークステーションの否認防止機能は、第三者的な立場で否認防止の判定を行う。

【0269】以下、図8を参照して、公開鍵暗号として楕円曲線暗号を用いた場合の否認防止部のソフト機能構成の実施例について説明する。

【0270】(1)ユーザ(がネットワークアクセスに用いる情報処理装置120)がデータMを送信するものとし、このユーザ120と接続するネットワーク通信管理用ワークステーション110に割り当てられた、ネットワークIDを $I_s$ 、これに対応する秘密鍵を $d_s$ 、公開鍵を $Q_s$ とする。

【0271】ユーザが否認防止を必要とする場合は、データMを入力するに際し否認防止要求801を入力する。

【0272】(2)通信管理セキュリティ機能f11は、データMには、ハッシュ関数と秘密鍵 $d_s$ により署名作成演算を実施し、署名データ $S_{ds}(M)$ を作成する。

【0273】これに、ネットワークIDである $I_s$ 、および、公開鍵 $Q_s$ を付加して、否認防止ファイル802を作成する。通信管理セキュリティ機能は、作成した否認防止ファイル802を、鍵管理用ワークステーション140の否認防止管理機能f41および送信相手先のネットワーク送受信管理機能f12に送付する。

【0274】(3)送信相手先の通信管理セキュリティ機能f11は、受信し復号して得られたデータにハッ



ジュ関数で処理したハッシュ値に識別子を付加し、これを鍵管理用ワークステーション140の否認防止機能f41に送付する。

【0275】(4) 鍵管理用ワークステーション140の否認防止機能f41は、送付された否認防止ファイル802および識別子の付加されたハッシュ値を、通信データの証拠として否認防止データベース26に登録し、一方、送付された署名データ $S_{ds}(M)$ 、付加された公開鍵 $Q_s$ 、およびハッシュ値 $E$ をもとに署名検証演算を実施し、この否認防止判定結果も、否認防止データベース26に登録する。

【0276】(5) 受信側のネットワーク通信管理用ワークステーション110も同様に、受信したデータと、署名データ $S_{ds}(M)$ および付加されて送付された公開鍵 $Q_s$ とにより署名検証演算を実施し、否認防止の確認を行う。

【0277】否認防止結果については、送信側のユーザにも伝達する。

【0278】(6) 受信側で実施した否認防止の確認結果についてトラブルが生じた場合、第三者的な立場の鍵管理用ワークステーション140に否認防止照会要求を行う。

【0279】否認防止管理機能f41は、否認防止照会要求を受けると、否認防止管理データベース26から否認防止判定結果を検索し、照会要求元に送付する。

【0280】次に、本発明のネットワーク通信システムにおいて、公開鍵暗号として楕円曲線暗号を用いた場合の鍵回復部のソフト機能の実施例について説明する。

【0281】図15の公開鍵暗号アルゴリズムによる暗号化通信処理部で示すように、データ $M$ の暗号化に用いるスクランブル鍵を $K_s$ 、デスクランブル鍵を $K_D$ とし、デスクランブル鍵を配送するためのセッション鍵としての公開鍵を $Q_{YID}$ とすると、暗号化通信は、暗号文 $E_{Ks}(M)$ と暗号化デスクランブル鍵 $E_{QYID}(K_D)$ の送信により実施される。

【0282】まず、信学技報 TECHNICAL REPORT OF IEICE ISEC97-15(1997-07)に「楕円曲線を利用した高速暗号化方法」宝木和夫、車谷博之に従って、暗号化デスクランブル鍵 $E_{QYID}(K_D)$ にしきい値ロジックを付加する鍵回復方式の実施例について説明する。

【0283】(1) 鍵管理用ワークステーション140(図4参照)の鍵回復機能f43(図4参照)において、鍵回復用の公開鍵 $Q_A, Q_B, Q_C$ を割り当て、公開するとともに、この公開鍵に対応する秘密鍵 $d_A, d_B, d_C$ ( $Q_A = d_A \cdot P, Q_B = d_B \cdot P, Q_C = d_C \cdot P$ )を保管するものとする。

【0284】暗号化デスクランブル鍵 $E_{QYID}(K_D)$ には、鍵 $Q_{YID}, Q_A, Q_B, Q_C$ で算出されるしきい値ロジックを付加するものとする。

【0285】(2) 共通鍵暗号を用いた場合と同様、暗号化通信を行う場合、デスクランブル鍵 $K_D$ を暗号化してからでないと、データをスクランブル鍵 $K_s$ で暗号化できないようにし、データの暗号文 $E_{Ks}(M)$ と暗号化デスクランブル鍵 $E_{QYID}(K_D)$ は必ずペアで生成されるようにする。

【0286】(3) 不測の事態が発生して暗号文を解読する必要がある場合、ペアとなった暗号文 $E_{Ks}(M), E_{QYID}(K_D)$ を鍵管理ワークステーション140(図4参照)に送付する。

【0287】鍵回復機能f43(図4参照)では、秘密鍵 $d_A, d_B, d_C$ の2つと、 $E_{QYID}(K_D)$ に付加されたしきい値ロジックを用いて復号し、デスクランブル鍵 $K_D$ を取得する。

【0288】次に、この鍵 $K_D$ で暗号文 $E_{Ks}(M)$ を復号し、データ $M$ を取得する。

【0289】本発明のネットワーク通信システムでは、送信するデータ $M$ の暗号文は、スクランブル鍵 $K_s$ による暗号化演算で作成される。

【0290】このため、共通鍵暗号を用いた鍵回復部(図9、図10参照)と全く同様に、スクランブル鍵 $K_s$ を $K_1, K_2$ の排他的論理和で表現し、これを用いて、鍵回復を実施する方法をとることもできる。図9、10に示す鍵回復用の鍵 $P_1, P_2$ は、共通鍵暗号アルゴリズムで運用することもできるが、鍵回復用として、公開鍵 $Q_A, Q_B$ により運用することも可能である。

【0291】この場合暗号文 $E_{Ks}(M)$ に鍵回復用として付加するデータは、 $K_1, K_2$ を公開鍵 $Q_A, Q_B$ により暗号化した暗号文 $E_{QA}(K_1), E_{QB}(K_2)$ であり、鍵回復は、鍵管理用ワークステーション140(図4参照)の鍵回復機能f43(図4参照)において公開鍵 $Q_A, Q_B$ に対応する秘密鍵 $d_A, d_B$ を用いて、付加されたデータを復号することにより実施する。

【0292】暗号処理装置17(図12参照)において公開鍵暗号を使用した場合における、暗号処理管理装置17(図12参照)、デスクランブル鍵同期装置22(図12参照)を運用するシーケンスは、公開鍵暗号でのスクランブル鍵の切り替えのシーケンスは、図16に示すようになる。

【0293】なお、公開鍵暗号を使用した場合、公開鍵はそのままセッション鍵として使用されるため、図12に描かれるセッション鍵復号化装置13は不要となる。ただし、セッション鍵署名検証装置を設置し、鍵管理用ワークステーションが実施した署名作成演算を検証し、セッション鍵の正当性を確認するものとする。

【0294】本発明のネットワーク通信システムでは、公開鍵暗号を用いた場合も共通鍵暗号を用いた場合と同様、ネットワーク通信管理用ワークステーションとこれと接続するユーザ(ユーザ用パーソナルコンピュータ)間で、1つの閉じたネットワークを構築することができ



る。

【0295】次に、図17を参照して、各情報の拠点に設置されたネットワーク管理用ワークステーションごとに、閉じたネットワークを構成する場合、公開鍵暗号を用いた鍵階層構造の実施例について説明する。

【0296】この場合も、ネットワーク通信管理用ワークステーション110<j>に $n_j$ 個のユーザが使用するパーソナルコンピュータが接続し、ネットワークを構成するものとする。

【0297】ユーザjのユーザIDを $ID_{ji}$ 、割り当てられた秘密鍵を $D_{ji}$ 、対応する公開鍵を $Q_{ji} (= d_{ji} \cdot P)$ とする。

【0298】ネットワーク通信管理用ワークステーション110<j>は、ユーザIDデータベースに $n_j$ 個のユーザID $\{ID_{j1}, ID_{j2}, \dots, ID_{jn_j}\}$ を登録し、ユーザ鍵管理データベースには、ユーザIDとユーザの公開鍵を対応させた $n_j$ 個のデータ $\{(ID_{j1}, Q_{j1}), (ID_{j2}, Q_{j2}), \dots, (ID_{ji}, Q_{ji}), \dots, (ID_{jn_j}, Q_{jn_j})\}$ を登録している。

【0299】ユーザ認証は、このネットワーク内で、図12に示す公開鍵暗号アルゴリズムによるユーザ認証方式で実施される。

【0300】各ネットワーク通信管理用ワークステーション110<j>には、ネットワークIDとして $IS_j$ 、秘密鍵 $d_{sj}$ 、および、これと対となる公開鍵 $Q_{sj} (= d_{sj} \cdot P)$ が割り当てられており、鍵管理用ワークステーション140は、ネットワークユーザIDデータベース25に、ネットワーク管理用ワークステーション110<j>のネットワークIDである $IS_j$ と、これが管理しているユーザのユーザID $\{ID_{j1}, ID_{j2}, \dots, ID_{jn_j}\}$ とを対応させて登録し、ネットワーク鍵構成データベース24には、ネットワークIDである $IS_j$ と、ネットワーク通信管理用ワークステーション110<j>の公開鍵 $Q_{sj}$ とを対応させた、 $m$ 個のデータ $\{(IS_1, Q_{s1}), (IS_2, Q_{s2}), \dots, (IS_m, Q_{sm})\}$ を登録している。ネットワーク通信管理用ワークステーション110<j>に属するユーザiが、暗号化通信を実施する手順も、共通鍵暗号アルゴリズムを用いた場合とほぼ同様である。

【0301】(1) ユーザiが、送信相手の宛先(名前)および送信するデータMを入力する。

【0302】(2) ネットワーク通信管理用ワークステーション110<j>は、鍵管理用ワークステーション140にセッション鍵発行要求を行う。

【0303】(3) 鍵管理用ワークステーション140の鍵構成管理機能f41(図4参照)は、ネットワークユーザIDデータベース25を検索し、送信相手の宛先(名前)から相手ユーザのユーザIDとして $ID_{ki}$ および相手ユーザが接続するネットワーク通信管理用ワーク

ステーション110<k>のネットワークIDとしての $IS_k$ を取得する。

【0304】次に、このネットワークIDである $IS_k$ をキーとしてネットワーク鍵構成データベース24を検索し、 $IS_k$ に対する公開鍵 $Q_{sk}$ を取得する。

【0305】(5) 鍵管理用ワークステーション140は、セッション鍵としての $Q_{sk}$ と送信相手先のネットワーク管理用ワークステーション110<k>のネットワークIDである $IS_k$ とを、要求元のネットワーク通信管理用ワークステーション110<j>に発行する。

【0306】(6) ネットワーク通信管理用ワークステーション110<j>は、セッション鍵 $Q_{sk}$ の発行を受け、スクランブル鍵 $K_s$ およびデスクランブル鍵 $K_D$ を生成する。

【0307】次に、データMをスクランブル鍵 $K_s$ で暗号化し、暗号文 $E_{ks}(M)$ を作成する。また、デスクランブル鍵 $K_D$ をセッション鍵 $Q_{sk}$ で暗号化し、暗号化デスクランブル鍵 $E_{Qsk}(K_D)$ を作成する。そこで、ネットワークIDである $IS_k$ をもとに、送信の相手先と通信系を接続し、作成した暗号文 $E_{ks}(M)$ 、暗号化デスクランブル鍵 $E_{Qsk}(K_D)$ を合成して送付する。

【0308】(7) 受信した相手先のネットワーク通信管理用ワークステーション110<k>は、割り当てられているマスター鍵としての秘密鍵 $d_{sk}$ で暗号化デスクランブル鍵 $E_{Qsk}(K_D)$ を復号し、デスクランブル鍵 $K_D$ を取得する。そして、このデスクランブル鍵 $K_D$ により暗号文 $E_{ks}(M)$ を復号し、データMを取得する。

【0309】次に、この復号したデータMを送信相手先のユーザが使用するパーソナルコンピュータなどの情報処理装置120に送付する。

【0310】以上の手順で、ネットワーク管理用ワークステーション110<j>に接続するユーザIDが $ID_{ji}$ のユーザから、ネットワーク管理用ワークステーション110<k>に接続するユーザIDが $ID_{ki}$ のユーザへの、暗号化通信が実施される。

【0311】本実施例で示すように、本ネットワーク通信システムの鍵管理用ワークステーションは、各ネットワーク通信管理用ワークステーションに割り付けられた公開鍵を管理し、各ユーザに割り付けられた公開鍵は、このユーザと接続しているネットワーク通信管理用ワークステーションで管理している。

【0312】ユーザ認証もこの鍵構成で実施でき、このことから、ネットワーク通信管理用ワークステーションとこれと接続しているユーザ間で1つの閉じたネットワークを構築していることがわかる。

【0313】各ユーザに割り当てられた秘密鍵と公開鍵は、ユーザ認証のみに用いられ、ネットワーク外部への暗号化通信に用いる鍵としては使用されないため、このネットワーク内では、独自の方式の暗号アルゴリズムを使用することも可能である。

【0314】この各ユーザに割り当てられた公開鍵でこのネットワーク内における暗号化通信を実施して、セキュリティを向上させることも可能である。

【0315】上記ネットワーク内においてユーザIDがID<sub>j</sub>iであるユーザからID<sub>j</sub>rであるユーザに暗号化通信を実施する手順を以下に示す。

【0316】(1) ユーザは、ID<sub>j</sub>iからユーザID<sub>j</sub>rへ暗号化通信を実施するためのセッション鍵の発行要求を接続するネットワーク通信管理用ワークステーション110<j>に送付する。

【0317】(2) ネットワーク通信管理用ワークステーション110<j>は、ユーザ固有鍵データベースを検索し、ユーザID<sub>j</sub>rに割り当てられた公開鍵Q<sub>j</sub>rを取得し、ユーザID<sub>j</sub>rに送付する。

【0318】(3) ユーザID<sub>j</sub>iは公開鍵Q<sub>j</sub>rにより送付するデータMを暗号化し、暗号文E<sub>Q<sub>j</sub>r</sub>(M)を作成し、ユーザID<sub>j</sub>rに送付する。

【0319】(4) 暗号文E<sub>Q<sub>j</sub>r</sub>(M)を受信したユーザID<sub>j</sub>rは、このユーザに割り当てられた公開鍵Q<sub>j</sub>rに対応する秘密鍵d<sub>j</sub>r(Q<sub>j</sub>r=d<sub>j</sub>r・P)を用いて暗号文を復号し、データMを取得する。

【0320】

【発明の効果】本発明によれば、複数のユーザで構成されるグループ群を双方向の通信ネットワークで結び、グループ間で構築した通信経路を利用して、各ユーザ間で情報を双方向に伝達するシステムにおいて、伝達する情報が変造、偽造、遺漏、不到達などの情報障害を受けないよう、安全性(セキュリティ)を確保することが可能となる。

【図面の簡単な説明】

【図1】 本発明を適用したネットワーク通信システムを示すネットワーク構成図である。

【図2】 本発明を適用したネットワーク通信システムを示すシステム構成図である。

【図3】 本発明を適用したネットワーク通信システムを示すブロック構成図である。

【図4】 本発明を適用したネットワーク通信システムの各ブロックにおけるソフト機能を示す機能ブロック図である。

【図5】 共通鍵暗号アルゴリズムを用いたアクセス管理部のソフト機能構成を示す説明図である。

【図6】 共通鍵暗号アルゴリズムを用いた暗号化通信処理部を示す説明図である。

【図7】 鍵管理部を示す説明図である。

【図8】 否認防止部を示す説明図である。

【図9】 鍵復号部における暗号化の処理を示すフロー図である。

【図10】 鍵復号部における復号化の処理を示すフロー図である。

【図11】 共通鍵暗号方式を適用した場合の階層構造

を示す説明図である。

【図12】 本発明を適用したネットワーク通信システムの暗号処理装置を示すブロック図である。

【図13】 共通鍵暗号方式を用いたスクランブル鍵の切り替え処理を示すフロー図である。

【図14】 公開鍵暗号アルゴリズムを用いたアクセス管理部のソフト構成を示す説明図である。

【図15】 公開鍵暗号アルゴリズムを用いた暗号化通信処理部を示す説明図である。

【図16】 公開鍵暗号方式を用いたスクランブル鍵の切り替え処理を示すフロー図である。

【図17】 公開鍵暗号方式の鍵の階層構造を示す説明図である。

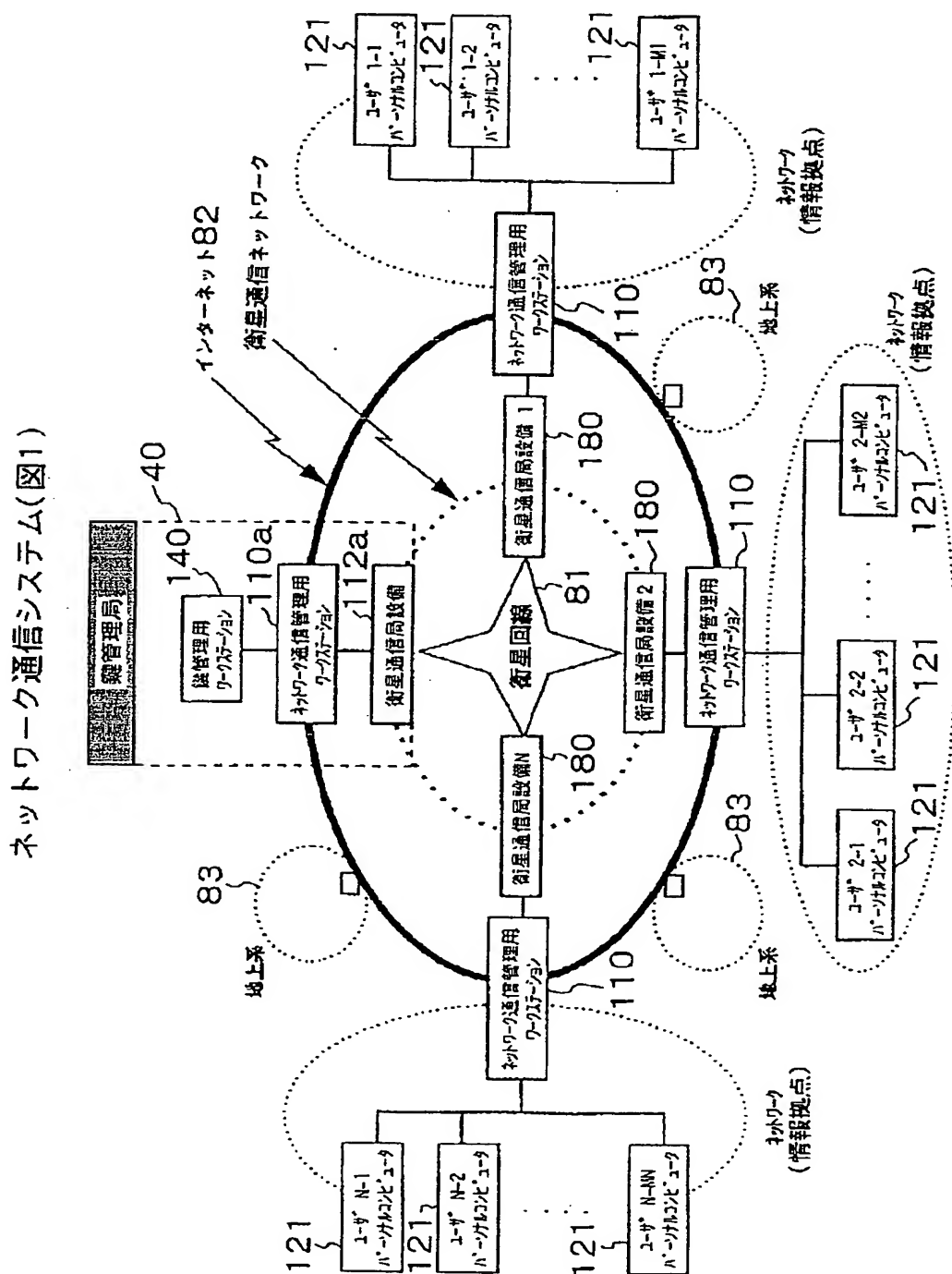
【符号の説明】

1…パーソナルコンピュータ、2…CPU、3…データ処理装置、5…CPU、6…データ処理装置、8…ユーザ認証用暗号装置、7…ユーザ認証用暗号装置、9…ICカード制御部、11…ユーザIDデータベース、12…ユーザ鍵管理データベース、13…セッション鍵復号化装置、15…デスクランブル鍵暗号化装置、16…スクランブル鍵/デスクランブル鍵生成装置、17…暗号処理管理装置、18…データ暗号化装置、19…合成装置、20…デスクランブル鍵復号化装置、22…デスクランブル鍵同期装置、21…分配装置、23…データ復号化装置、24…ネットワーク鍵構成データベース、25…ネットワークユーザIDデータベース、26…否認防止管理データベース、27…ネットワークIDデータベース、28…ユーザIDデータベース、40…鍵管理局、81…衛星回線、82…インターネット、83…地上回線、110<1>…<N>、110a、110…ネットワーク通信管理用ワークステーション、120<1>…<1-M1>…<N-MN>、120…情報処理装置、121…パーソナルコンピュータ、122…CAD用ワークステーション、123…TV会議用パーソナルコンピュータ、124…メールサーバ、130…ローカルエリアネットワーク、180…衛星通信局設備、181…ルータ、501…アクセス要求、502…認証要求、503…ユーザ認証要求、504…ユーザマスタ鍵、505…シーケンス番号、506…ユーザID、507、510…チャレンジコード、508…ユーザマスタ鍵、509…暗号化チャレンジコード、601…セッション鍵、602…送信側のユーザのマスタ鍵、603…受信側のユーザのマスタ鍵、604、605…暗号文、606…スクランブル鍵、607…デスクランブル鍵、608、609…暗号文、701…セッション鍵発行要求、702…発行されたセッション鍵、703…マスタ鍵更新要求、801…否認防止要求、802、803…否認防止ファイル、1010…アクセス管理部、1020…ネットワーク通信管理部、1030…暗号化通信処理部、1040…鍵管理部、1050…否認

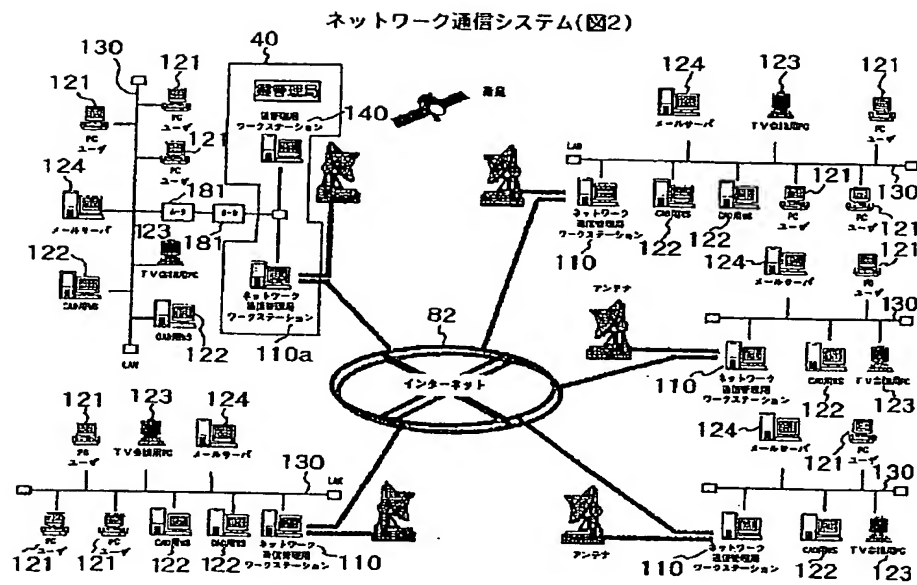
防止管理部、1060…鍵回復部、1501…スクランブル鍵、1502、1503…デスクランブル鍵、1504、1505…データ、1506…暗号文、1507…公開鍵、1508…暗号化デスクランブル鍵、1510…ユーザのマスター鍵としての秘密鍵、f11…通信管理セキュリティ機能、f12…ネットワーク送受信管

理機能、f 1 3…スクランブル機能、f 1 4…デスクランブル機能、f 1 5…通信構成管理機能、f 2 1…ユーザセキュリティ機能、f 2 2…データファイル処理機能、f 4 1…鍵構成管理機能、f 4 2…否認防止機能、f 4 3…鍵回復機能。

【図 1】

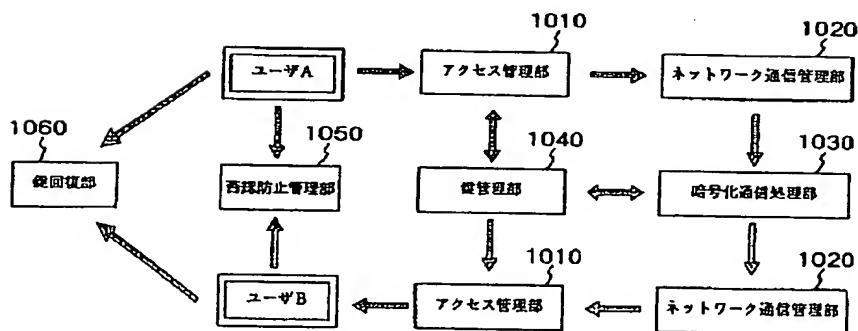


【図2】



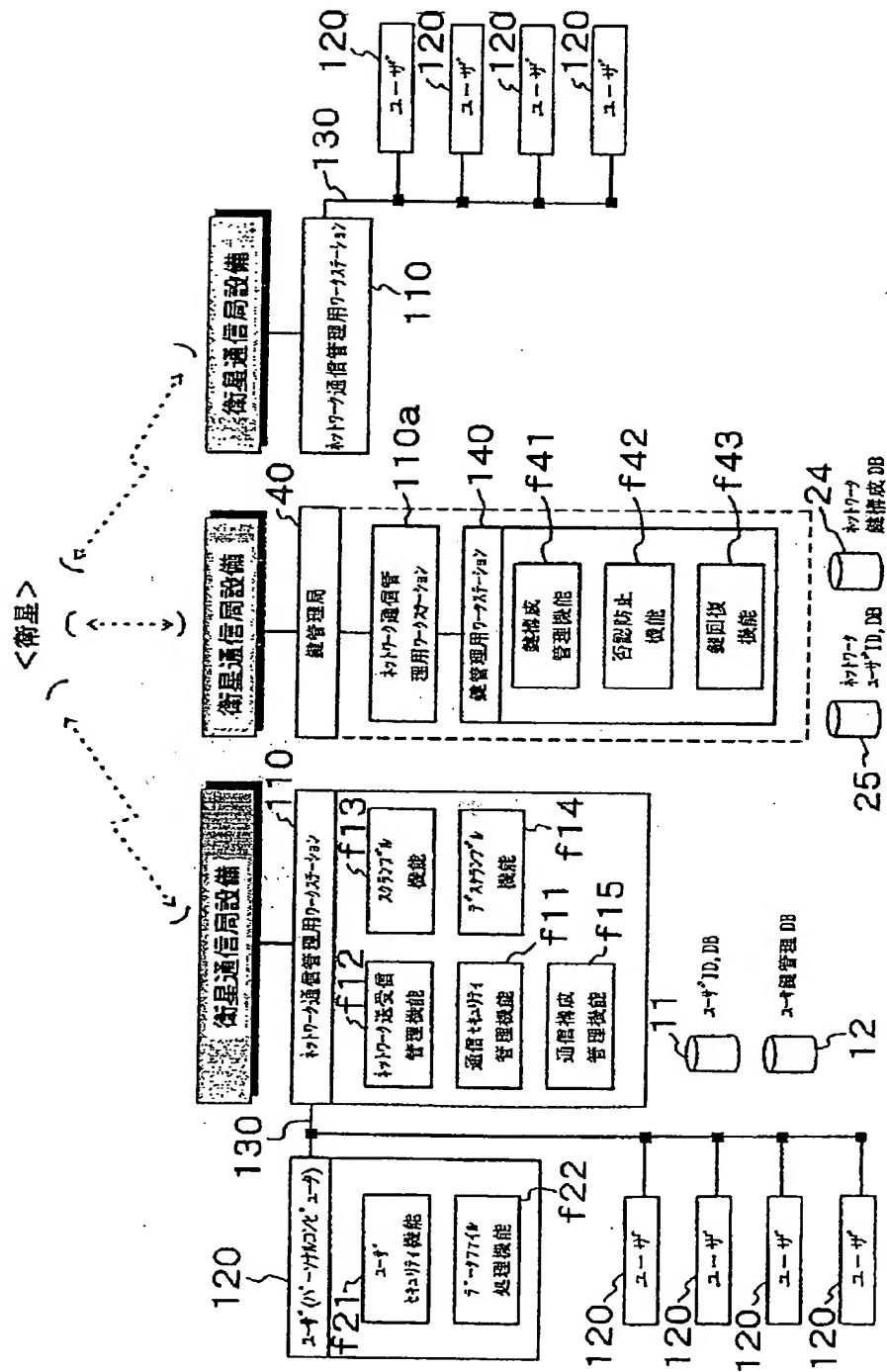
【図3】

ネットワーク通信システムの制御処理部の構成(図3)



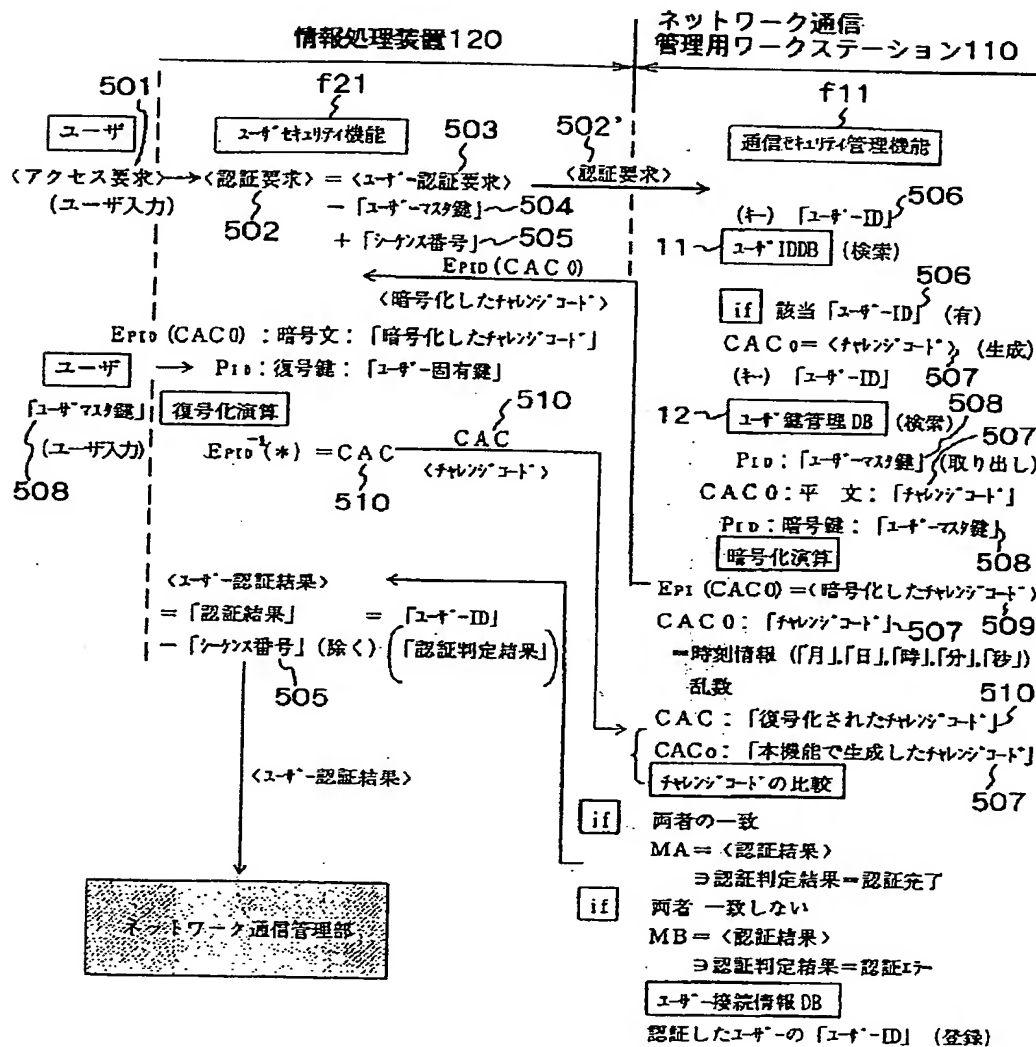
【図4】

ネットワーク通信システムに組み込まれるソフト機能(図4)



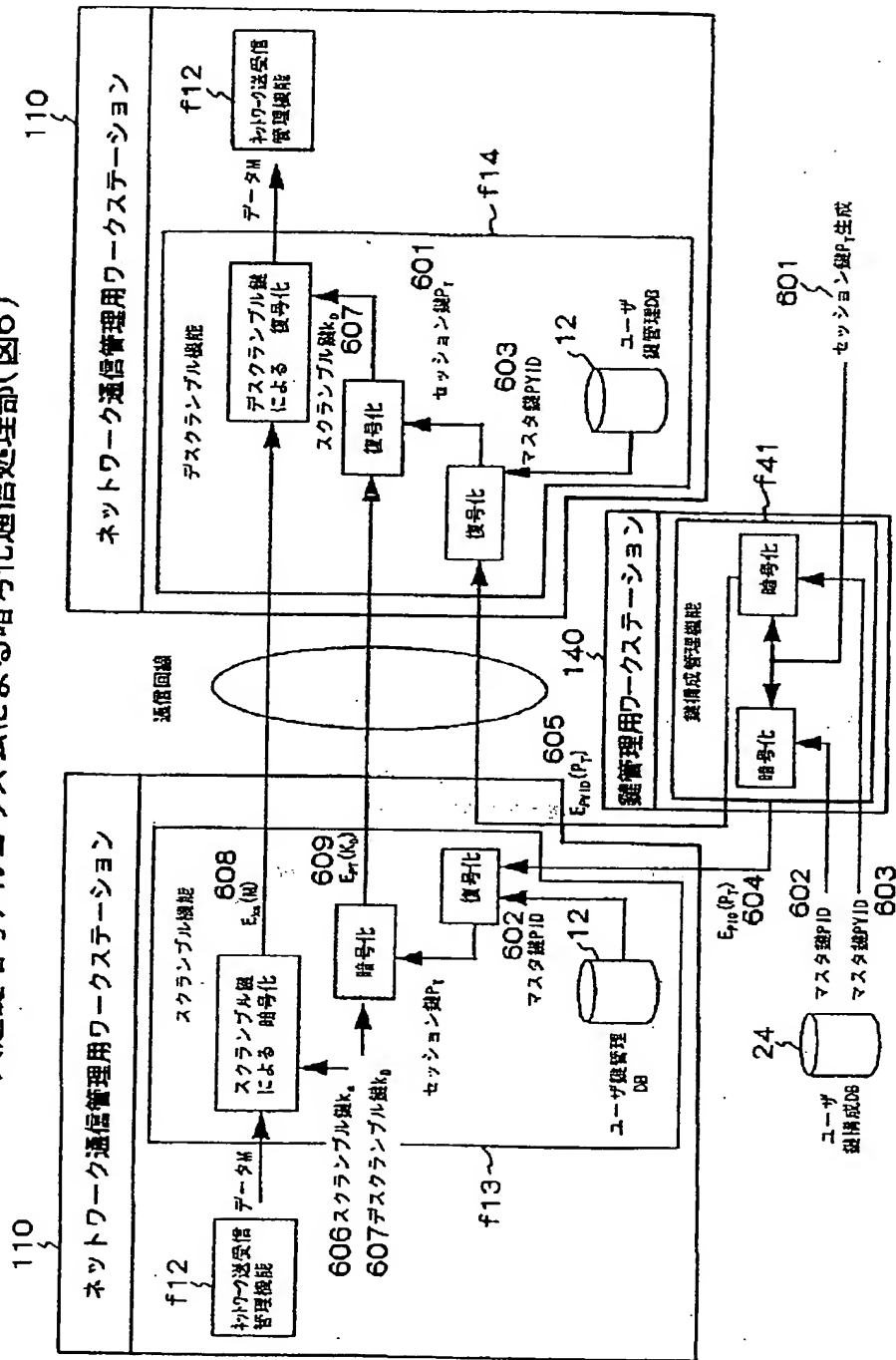
【図5】

共通鍵暗号アルゴリズムによるアクセス管理部のソフト機能構成  
(図5)



【図6】

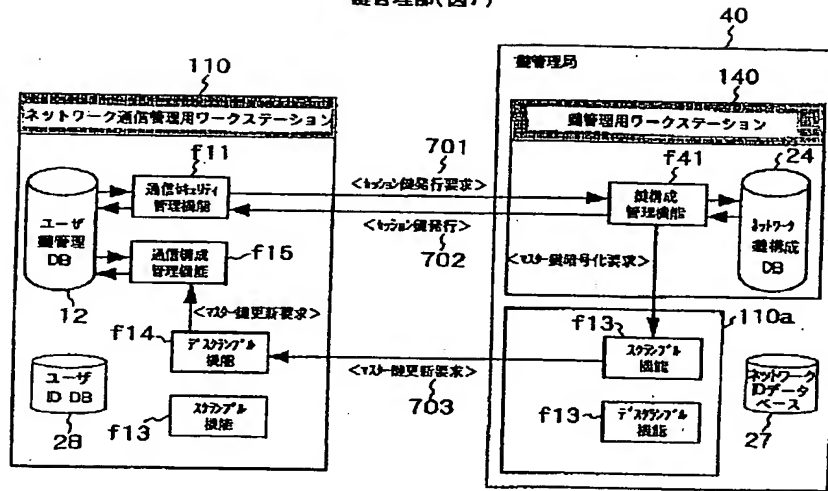
共通鍵暗号アルゴリズムによる暗号化通信処理部(図6)





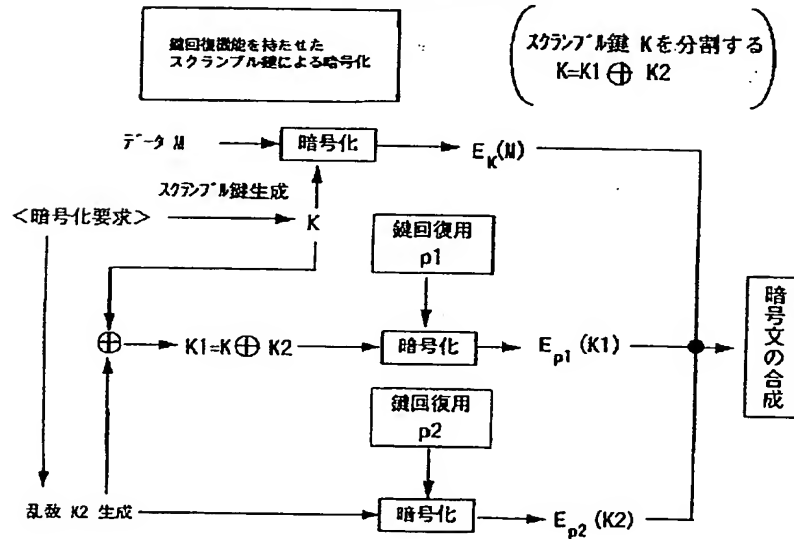
【図7】

鍵管理部(図7)



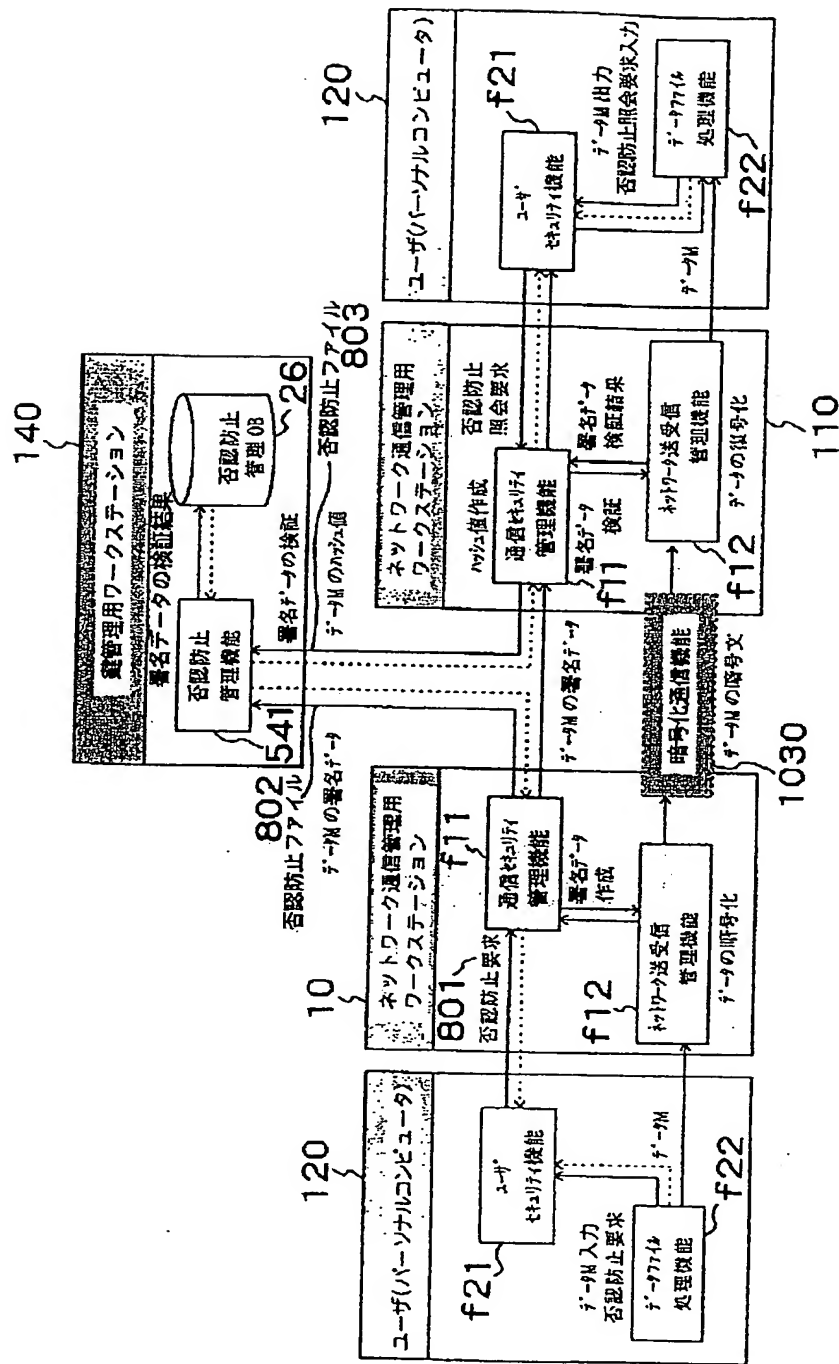
【図9】

鍵回復部(暗号化)(図9)



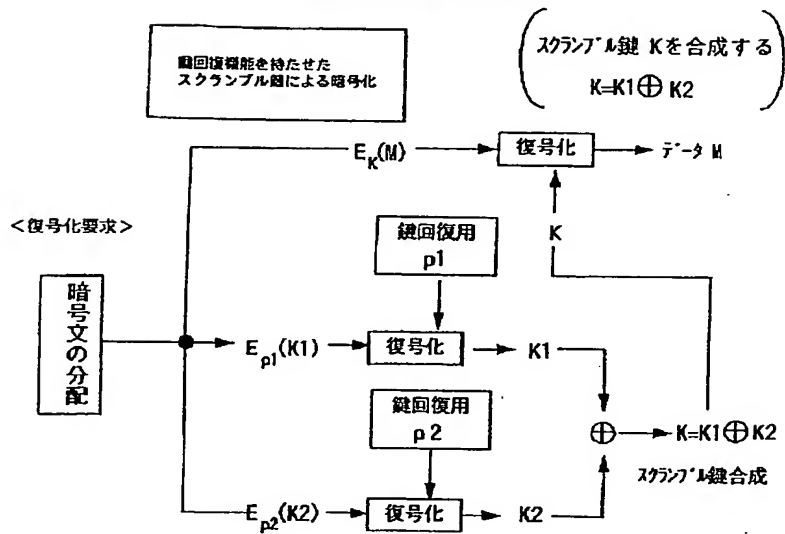
【図8】

## 否認防止部(図8)



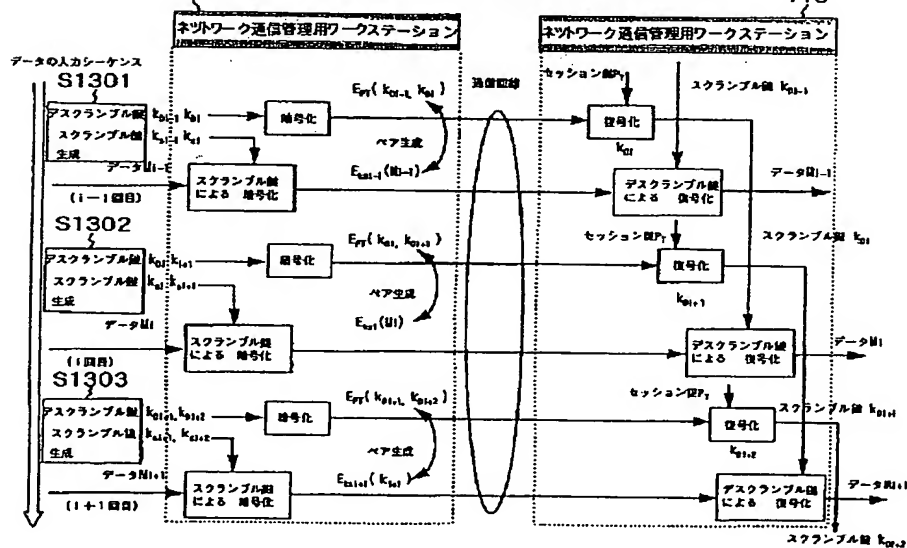
【図 10】

### 縫回復部(複号化)(図10)

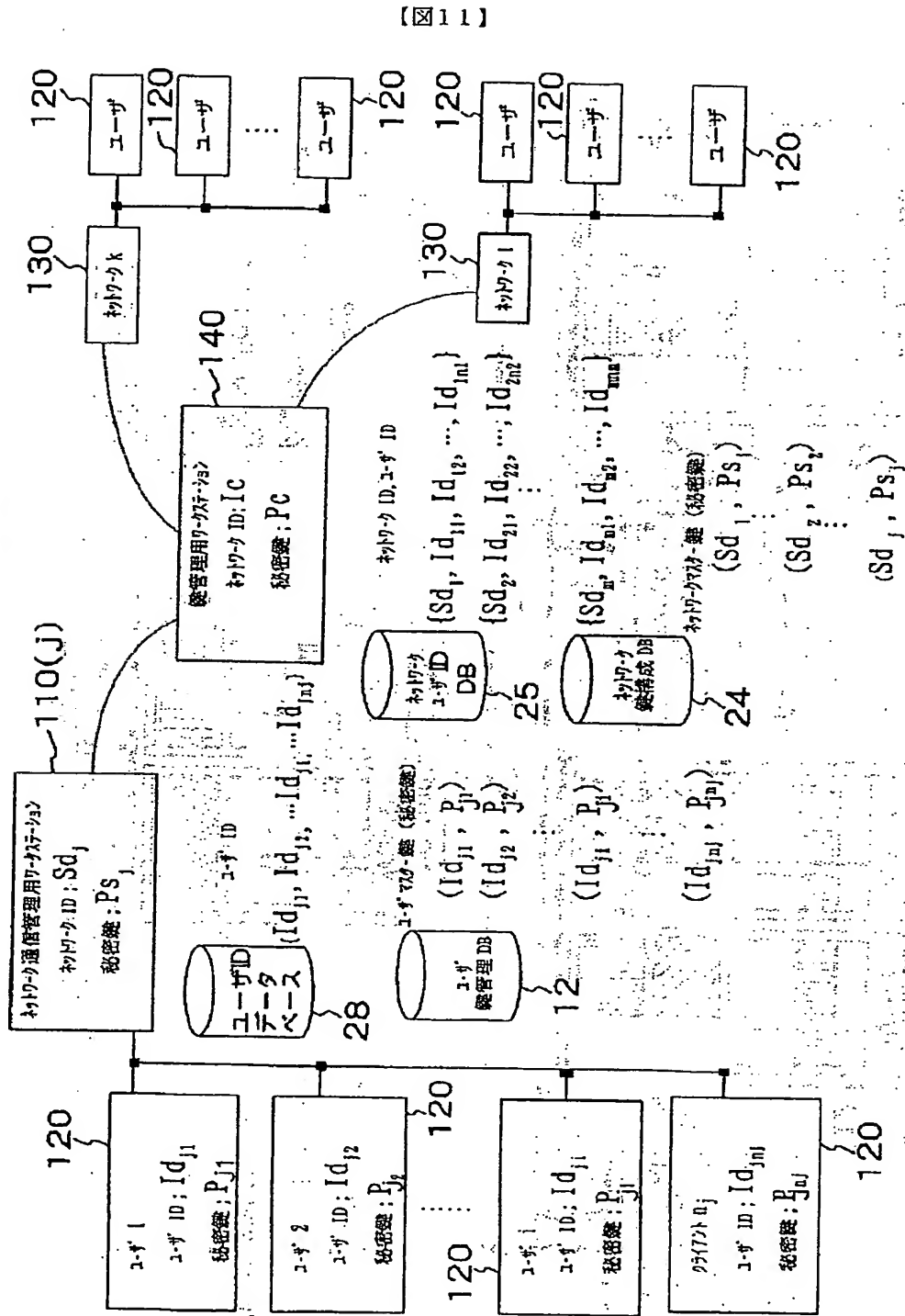


【图13】

110 共通鍵暗号でのスクランブル鍵の切り替え(図13)



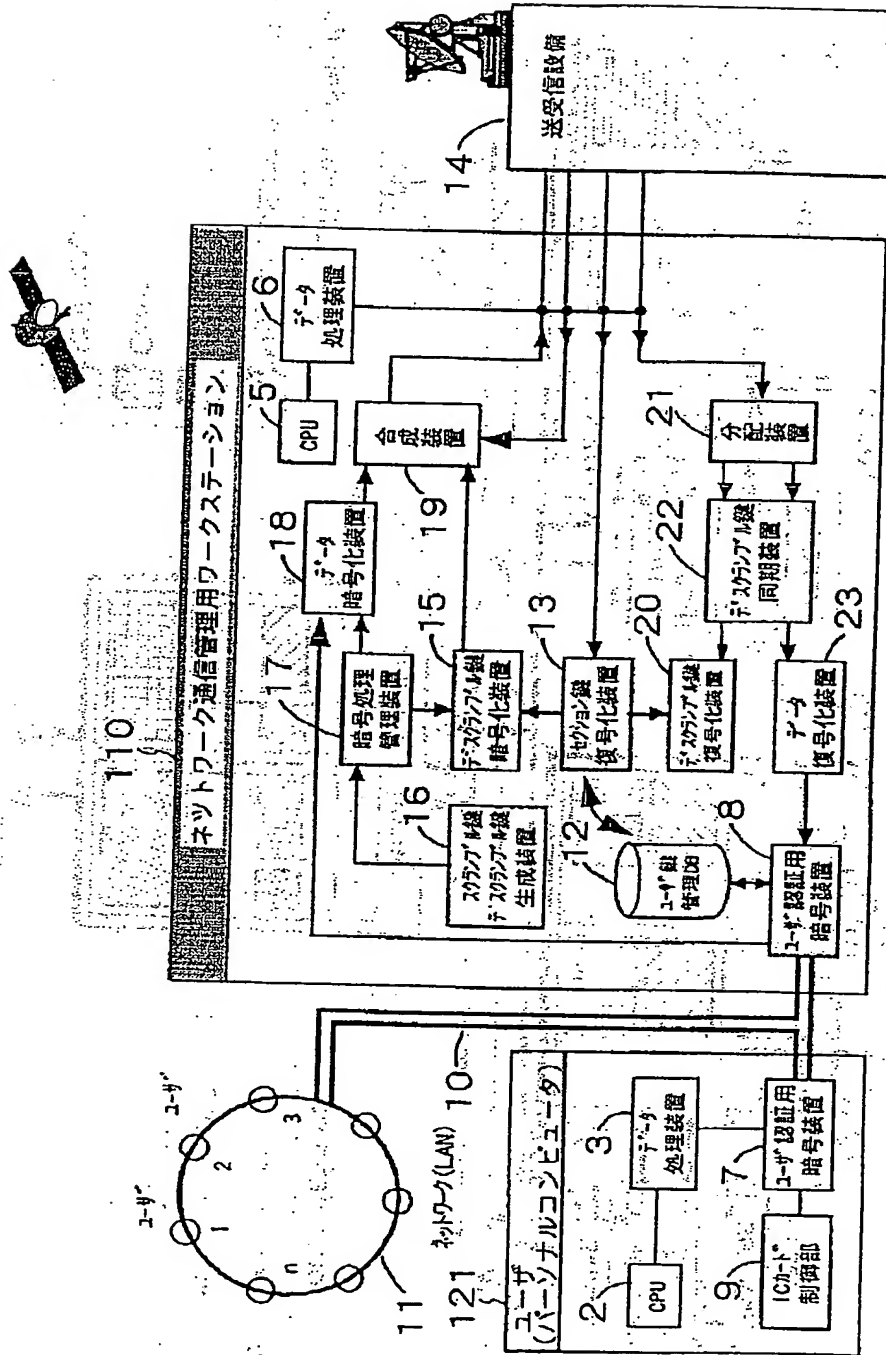
共通鍵暗号方式の鍵の階層構造(図11)



【図11】

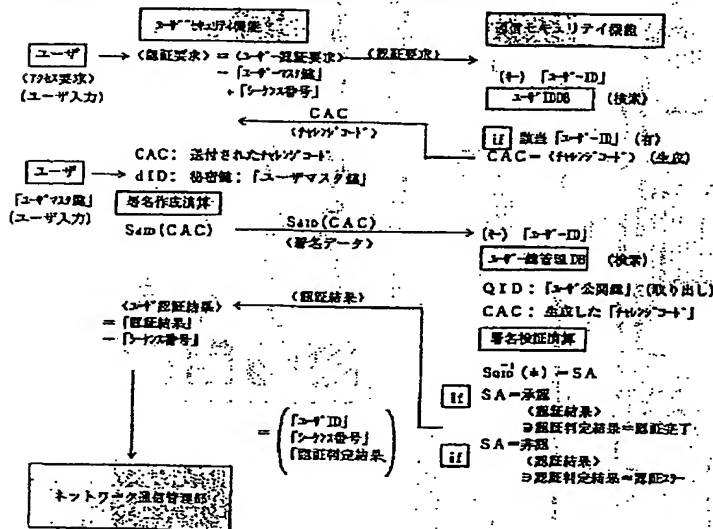
【図12】

ネットワーク通信システムの暗号処理装置(図12)



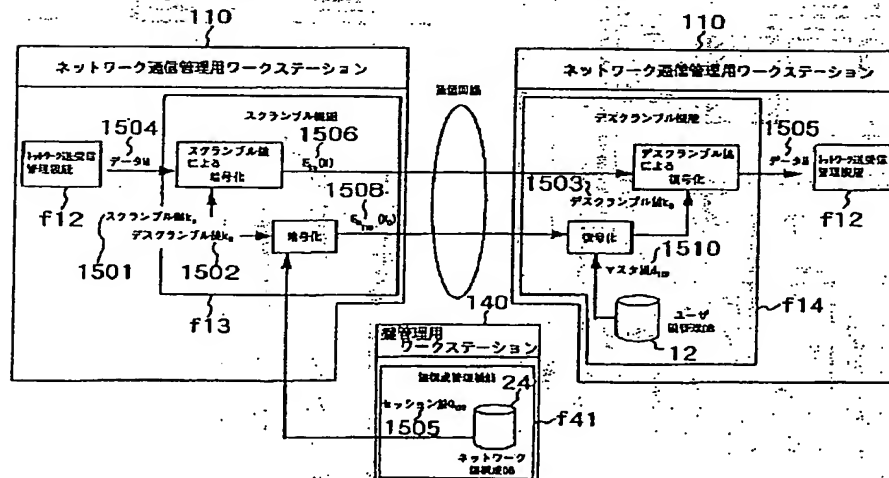
【図14】

公開鍵暗号アルゴリズムによるアクセス管理部のソフト機能構成(図14)

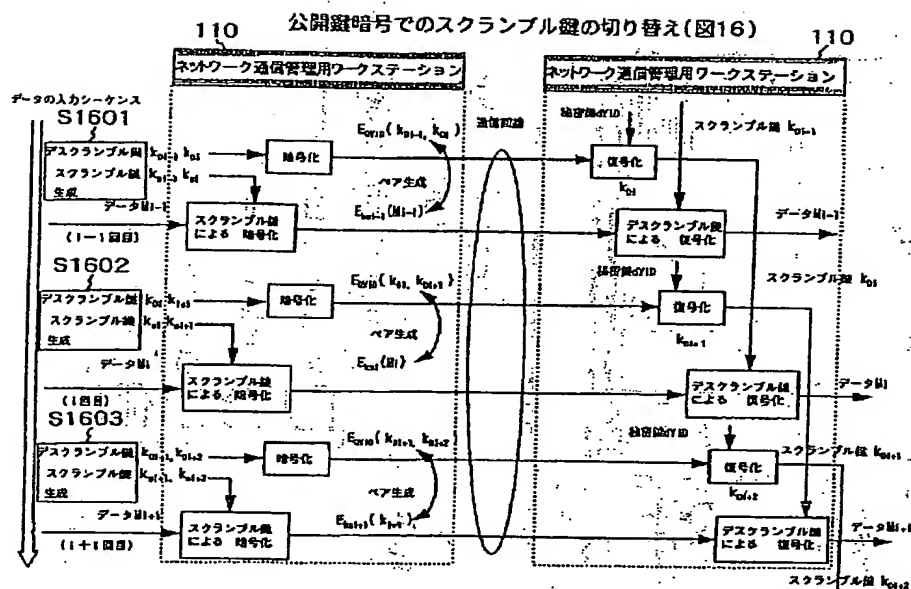


【図15】

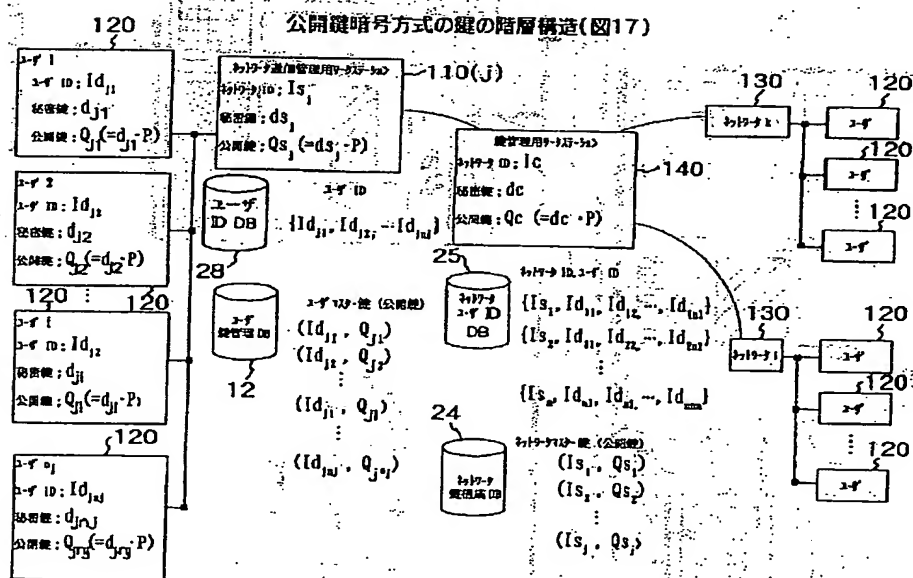
公開鍵暗号アルゴリズムによる暗号化通信処理部(図15)



【图 16】



【图 1-7】



フロントページの続き

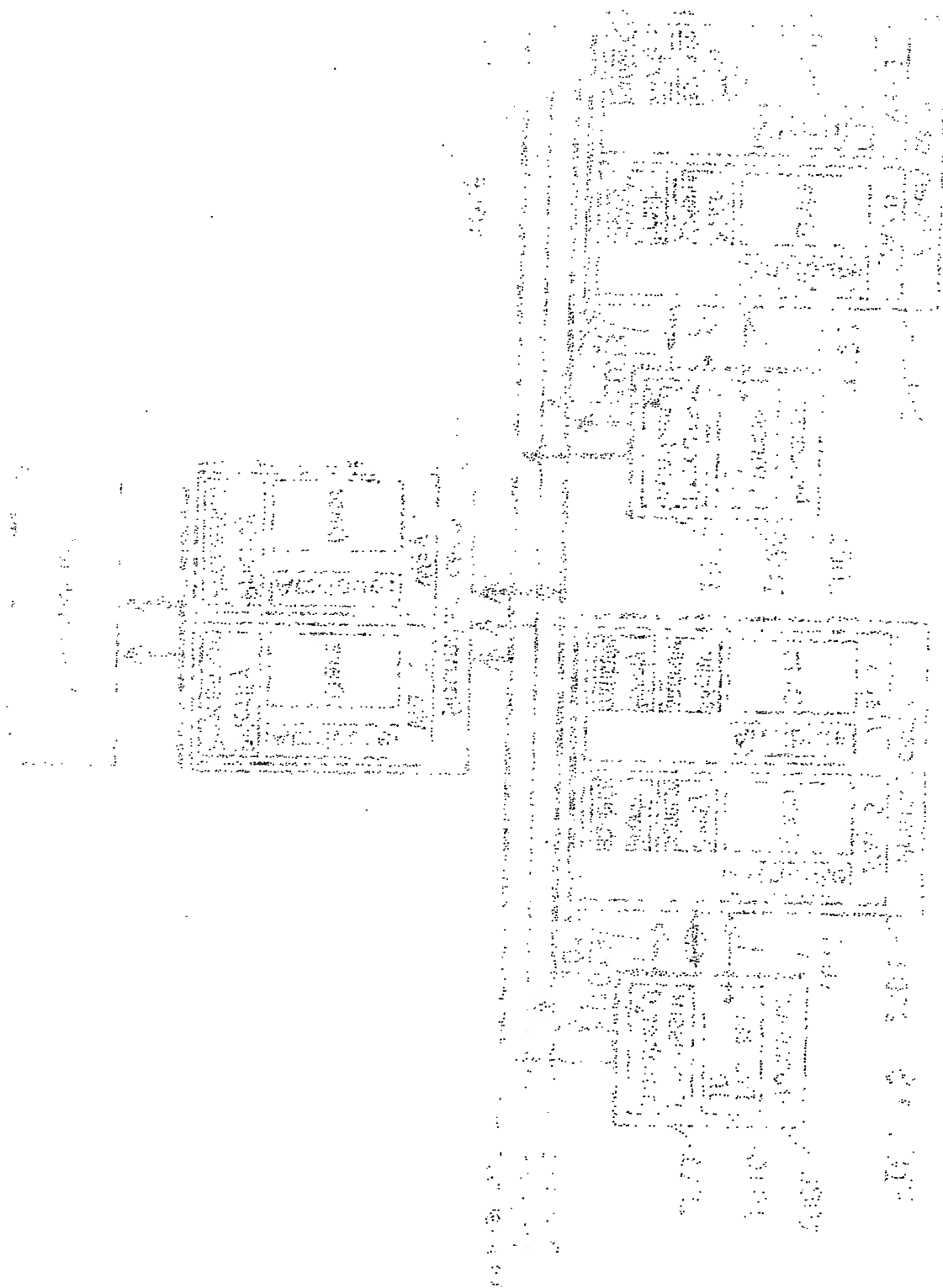
(72)発明者 速水 洋志  
神奈川県横浜市戸塚区戸塚町216番地 株  
式会社日立製作所宇宙技術推進本部内

(72)発明者 谷口 英宣  
神奈川県横浜市戸塚区戸塚町216番地 株  
式会社日立製作所宇宙技術推進本部内



(72)発明者 白木 光彦

神奈川県横浜市戸塚区戸塚町216番地 株  
式会社日立製作所宇宙技術推進本部内



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☒ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☒ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**